Wi-Fi 安全访问 2 (WPA 2) 配置示例

目录

简介

本文档介绍了在无线局域网 (WLAN) 中使用 Wi-Fi 保护访问 2 (WPA 2) 的优点。本文档提供了有关如何在 WLAN 中实施 WPA 2 的两个配置示例。第一个示例显示了如何在企业模式下配置 WPA 2，第二个示例在个人模式下配置了 WPA 2。

注意： WPA与可扩展的认证协议(EAP)一起使用。

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
- 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 Aironet 无

线局域网安全概述。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Aironet 1310G运行Cisco IOS软件版本12.3(2)JA的接入点(AP) /Bridge
- 运行固件版本 2.5 的 Aironet 802.11a/b/g CB21AG 客户端适配器
- Aironet Desktop软件(ADU)该运行固件2.5

注意： Aironet CB21AG 和 PI21AG 客户端适配器软件与其他 Aironet 客户端适配器软件不兼容。您必须以CB21AG和PI21AG卡使用ADU，并且您必须使用Aironet客户端工具(ACU)其他Aironet客户端适配器。有关如何安装 CB21AG 卡和 ADU 的详细信息，请参阅安装客户端适配器。

注意： 本文档使用具有集成天线的 AP/网桥。如果使用需要外部天线的 AP/网桥，请确保已将天线连接到 AP/网桥。否则，AP/网桥将无法连接到无线网络。某些 AP/网桥型号附带集成天线，而其他型号则需要外部天线才能进行常规操作。有关附带内部或外部天线的 AP/网桥型号的信息，请参阅相应设备的订购指南/产品指南。

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

WPA 是一个来自 Wi-Fi 联盟的基于标准的安全解决方案，用于解决本地 WLAN 中的漏洞。WPA 为 WLAN 系统提供增强的数据保护和访问控制。WPA针对在原始IEEE 802.11安全实施的所有已知有线等效保密(WEP)漏洞并且给在企业和小型办公室、家庭办公室环境的WLAN带来一个立即安全问题解决方案。

WPA2 是新一代 Wi-Fi 安全证书。WPA 2 是 Wi-Fi 联盟对承认的 IEEE 802.11i 标准的可互操作实施。WPA2 通过将计数器模式与口令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) 推荐的高级加密标准 (AES) 加密算法。AES 计数器模式是一次使用一个 128 位加密密钥加密 128 位数据块的块加密程序。CCMP算法导致消息完整性代码(MIC)该提供数据来源验证和数据完整性无线帧的。

注意： CCMP 也称为 CBC-MAC。

因为AES比临时密钥完整性协议(TKIP)，提供强加密WPA2比WPA提供高水平安全。TKIP 是 WPA 使用的加密算法。WPA 2 在每个关联上创建新的会话密钥。用于网络上各个客户端的加密密钥都是唯一的，并且特定于该客户端。最终，通过空气发送的每个数据包都会使用一个唯一的密钥进行加密。使用新的唯一加密密钥会增强安全性，这是因为不存在密钥重用。WPA 仍然被认为是安全的，TKIP 也尚未被破解。但是，Cisco 建议客户尽快转换到 WPA 2。

WPA 和 WPA 2 都支持两种操作模式：

- 企业模式
- 个人模式

本文档将讨论如何使用 WPA 2 实施这两个模式。

Cisco Aironet 设备的 WPA 2 支持

以下设备支持 WPA 2：

- Aironet 1130AG AP 系列和 1230AG AP 系列
- Aironet 1100 AP 系列
- Aironet 1200 AP 系列
- Aironet 1300 AP 系列

注意： 用 802.11g 无线电装置装备这些 AP，并使用 Cisco IOS 软件版本 12.3(2)JA 或更高版本。

以下设备也支持 WPA 2 和 AES：

- 部件号为 AIR-RM21A 和 AIR-RM22A 的 Aironet 1200 系列无线电模块**注意：** 部件号为 AIR-RM20A 的 Aironet 1200 无线电模块不支持 WPA 2。
- 具有固件版本 2.5 的 Aironet 802.11a/b/g 客户端适配器

注意： Cisco Aironet 350 系列产品不支持 WPA 2，因为其无线电装置缺少 AES 支持。

注意： Cisco Aironet 1400 系列无线网桥不支持 WPA 2 或 AES。

在企业模式下配置

期限**企业模式**是指测试是相互可操作的在验证的预先共享密钥的产品(PSK)和IEEE 802.1x操作模式。由于 802.1x 在支持各种身份验证机制方面的灵活性及其更强大的加密算法，它被认为比任何一个传统身份验证框架都安全。企业模式下的 WPA 2 分两个阶段执行身份验证。开放式身份验证的配置发生在第一阶段。第二阶段是使用 EAP 方法之一进行 802.1x 身份验证。AES 提供了加密机制。

在企业模式，客户端和认证服务器互相验证与使用EAP验证方法，并且客户端和服务器成对地生成一主密钥(PMK)。服务器使用 WPA 2 动态地生成 PMK，并将 PMK 传送到 AP。

本部分讨论在企业操作模式下实施 WPA 2 所需的配置。

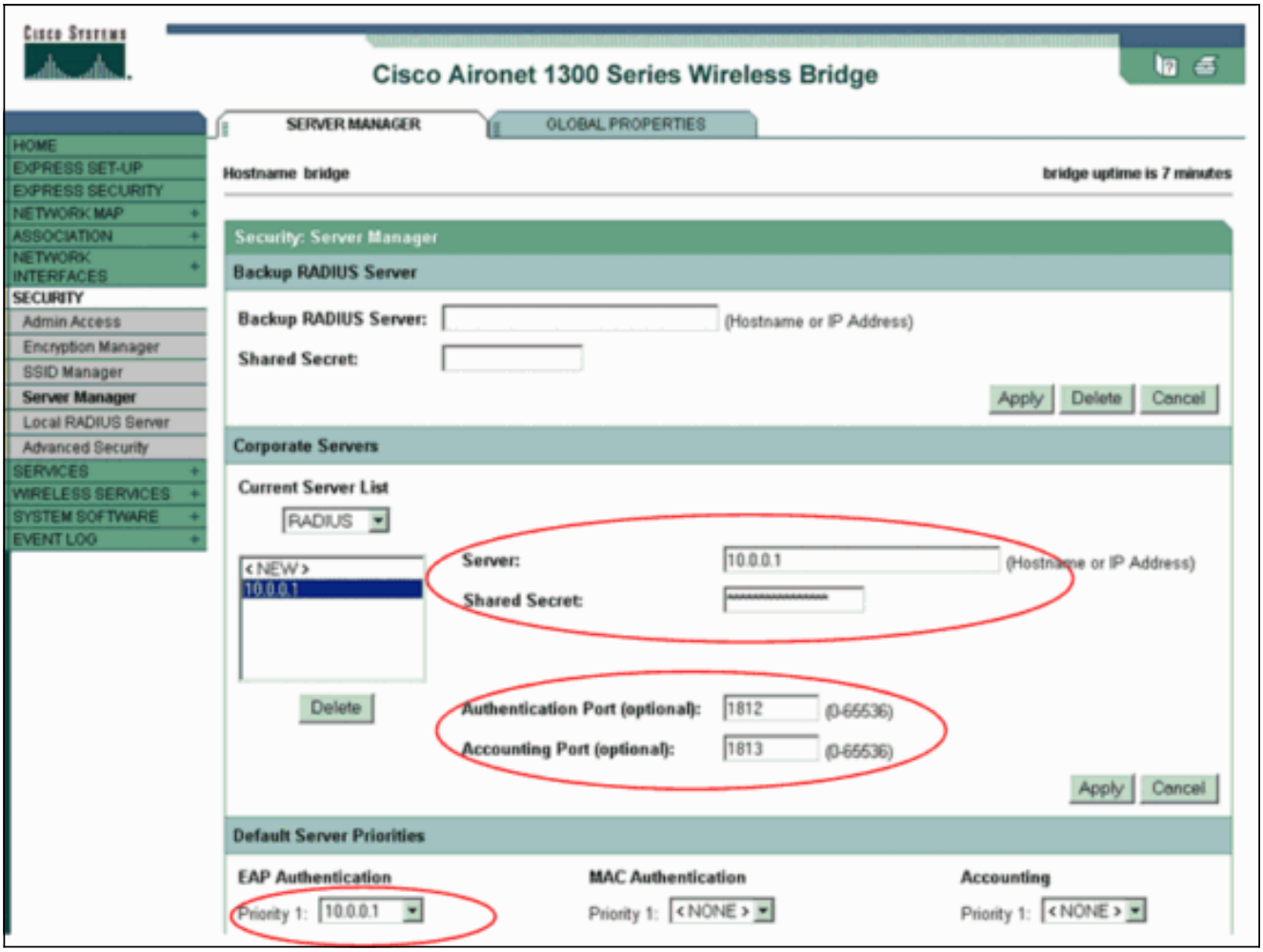
网络设置

在运行的此设置， Aironet 1310G AP/bridge思科轻量级扩展身份认证协议(LEAP)验证一个用户用 WPA 2兼容客户端适配器。使用配置了 AES-CCMP 加密的 WPA 2 时会发生密钥管理。将 AP 配置为运行 LEAP 身份验证的本地 RADIUS 服务器。要实施此设置，必须配置客户端适配器和 AP。配置 AP 和配置客户端适配器部分显示了 AP 和客户端适配器上的配置。

配置 AP

使用 GUI 完成以下配置 AP 的步骤：

1. 将 AP 配置为运行 LEAP 身份验证的本地 RADIUS 服务器。在左侧菜单中选择 **Security > Server Manager**，并定义 RADIUS 服务器的 IP 地址、端口和共享密钥。由于此配置将 AP 配置为本地 RADIUS 服务器，因此请使用 AP 的 IP 地址。将端口 1812 和 1813 用于本地 RADIUS 服务器操作。在 Default Server Priorities 区域中，将默认优先进行 EAP 身份验证的服务器定义为 10.0.0.1。**注意：** 10.0.0.1 为本地 RADIUS 服务器。

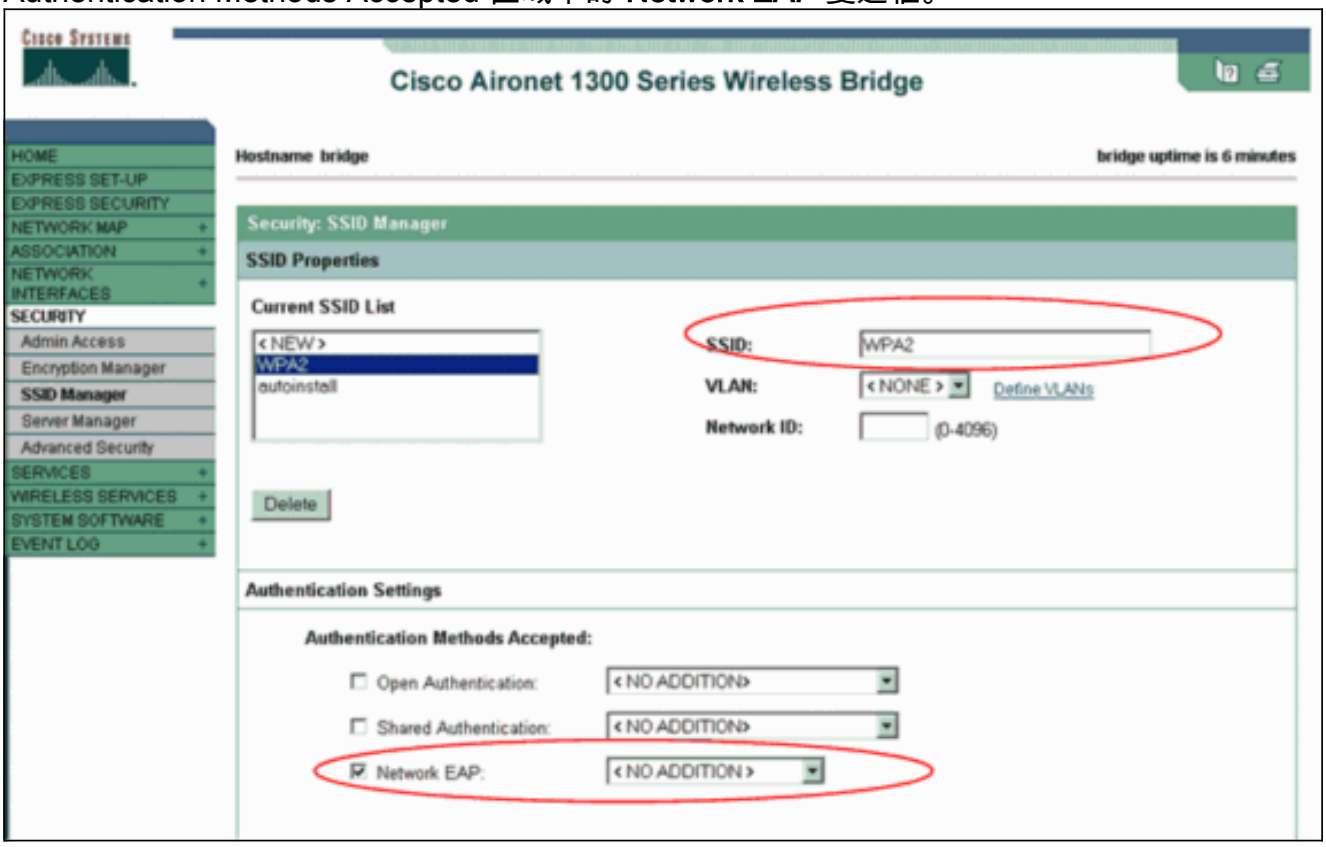


2. 从左侧菜单中选择 **Security > Encryption Manager**，并完成以下步骤：在 Cipher 菜单中，选择 **AES CCMP**。此选项通过将计数器模式和 CBC-MAC 结合使用来启用 AES 加密。

单击 **Apply**。

3. 选择**安全> SSID管理器**并且创建一新的服务集标识(SSID)为了用在WPA2上。选中

Authentication Methods Accepted 区域中的 **Network EAP** 复选框。

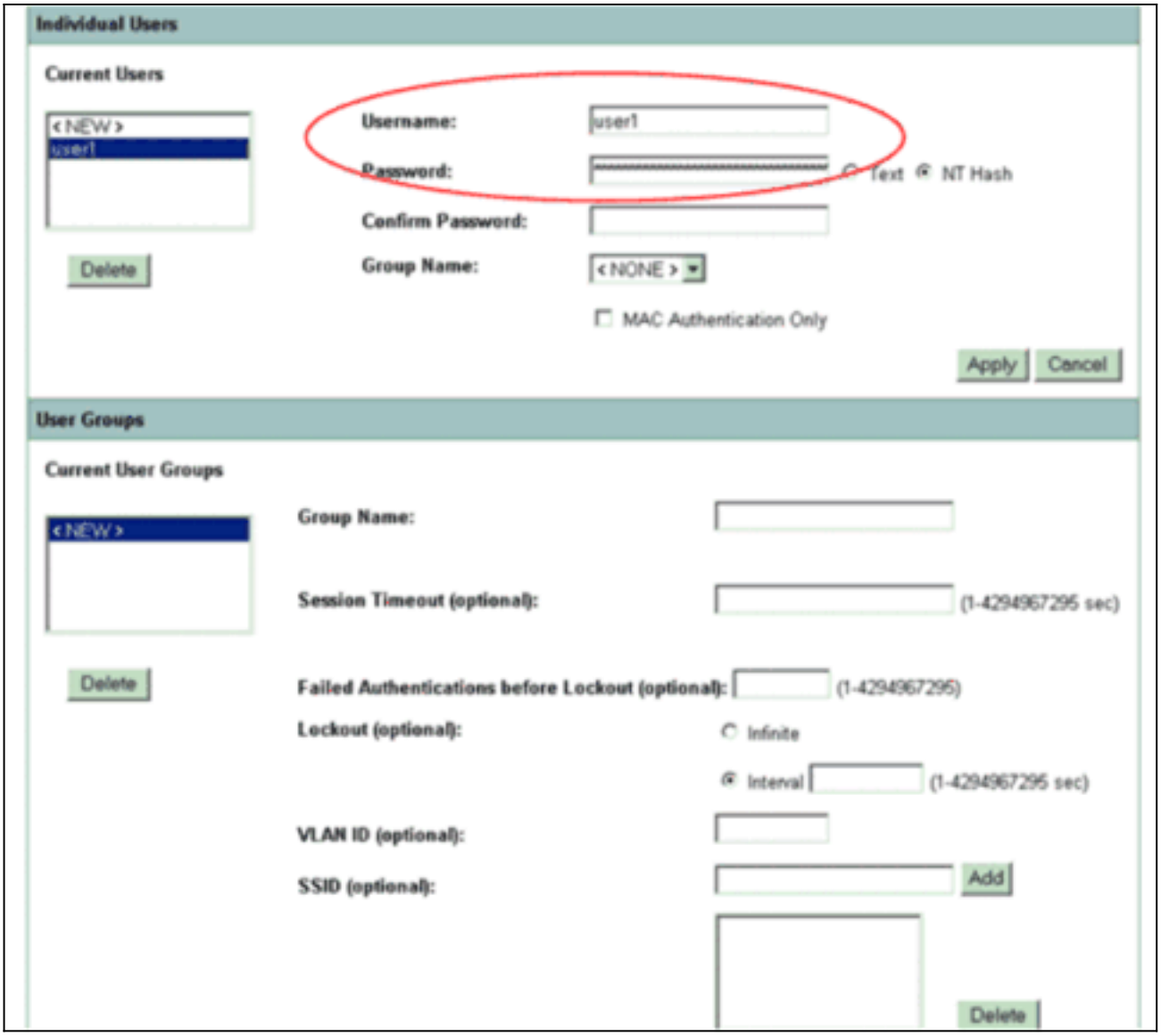


注意： 在无线电接口上配置身份验证类型时，请使用以下准则：Cisco 客户端 - 使用 Network EAP。第三方客户端（包括与 Cisco Compatible Extensions [CCX] 兼容的产品）- 使用采用 EAP 的开放式身份验证。Cisco 客户端与第三方客户端的组合 - 同时选择 Network EAP 和 Open Authentication with EAP。将 Security SSID Manager 窗口向下滚动到 Authenticated Key Management 区域，并完成以下步骤：在 Key Management 菜单中，选择 **Mandatory**。选中右侧的 **WPA** 复选框。单击 **Apply**。**注意：** VLAN 的定义是可选的。如果定义了 VLAN，则与此 SSID 的使用关联的客户端设备将被划分到 VLAN 中。有关如何实施 VLAN 的详细信息，请参阅配置 VLAN。

4. 选择 **Security > Local Radius Server**，并完成以下步骤：单击位于窗口顶部的 **General Set-Up** 选项卡。选中 **LEAP** 复选框，并单击 Apply。在 Network Access Servers 区域中，定义 RADIUS 服务器的 IP 地址和共享密钥。对于本地 RADIUS 服务器，请使用 AP 的 IP 地址。

单击 **Apply**。

5. 将 General Set-Up 窗口向下滚动到 Individual Users 区域，然后定义各个用户。用户组的定义是可选的。



此配置定义了名为“user1”的用户并定义了口令。此外，此配置还为口令选择了 NT 散列。完成本部分中的过程后，AP 将准备接受来自客户端的身份验证请求。下一步是配置客户端适配器。

CLI 配置

接入点

```
ap#show running-config Building configuration... . . .
aaa new-model !--- This command reinitializes the
authentication, !--- authorization and accounting
functions. ! ! aaa group server radius rad_eap server
10.0.0.1 auth-port 1812 acct-port 1813 !--- A server
group for RADIUS is created called "rad_eap" !--- that
uses the server at 10.0.0.1 on ports 1812 and 1813. . .
. aaa authentication login eap_methods group rad_eap !--
- Authentication [user validation] is to be done for !--
- users in a group called "eap_methods" who use server
group "rad_eap". . . . ! bridge irb ! interface
Dot11Radio0 no ip address no ip route-cache ! encryption
vlan 1 key 1 size 128bit 12345678901234567890123456
transmit-key !---This step is optional !--- This value
seeds the initial key for use with !--- broadcast
[255.255.255.255] traffic. If more than one VLAN is !---
used, then keys must be set for each VLAN. encryption
vlan 1 mode wep mandatory !--- This defines the policy
for the use of Wired Equivalent Privacy (WEP). !--- If
```

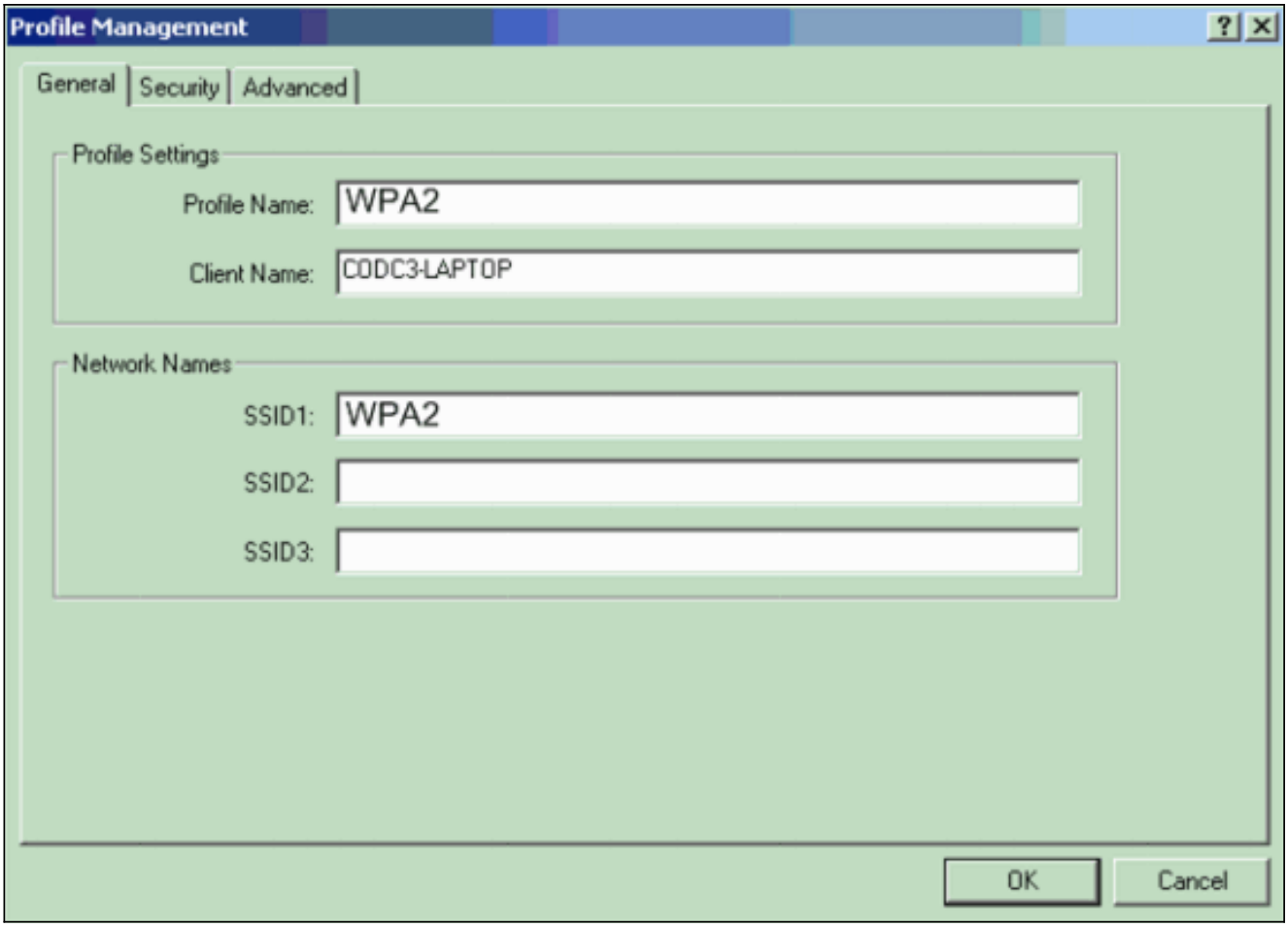
```
more than one VLAN is used, !--- the policy must be set
to mandatory for each VLAN. broadcast-key vlan 1 change
300 !--- You can also enable Broadcast Key Rotation for
each vlan and Specify the time after which Brodacst key
is changed. If it is disabled Broadcast Key is still
used but not changed. ssid cisco vlan 1 !--- Create a
SSID Assign a vlan to this SSID authentication open eap
eap_methods authentication network-eap eap_methods !---
Expect that users who attach to SSID "cisco" !---
request authentication with the type 128 Open EAP and
Network EAP authentication !--- bit set in the headers
of those requests, and group those users into !--- a
group called "eap_methods." ! speed basic-1.0 basic-2.0
basic-5.5 basic-11.0 rts threshold 2312 channel 2437
station-role root bridge-group 1 bridge-group 1
subscriber-loop-control bridge-group 1 block-unknown-
source no bridge-group 1 source-learning no bridge-group
1 unicast-flooding bridge-group 1 spanning-disabled . .
. interface FastEthernet0 no ip address no ip route-
cache duplex auto speed auto bridge-group 1 no bridge-
group 1 source-learning bridge-group 1 spanning-disabled
! interface BVI1 ip address 10.0.0.1 255.255.255.0 !---
The address of this unit. no ip route-cache ! ip
default-gateway 10.77.244.194 ip http server ip http
help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server local !--- Engages the Local RADIUS Server
feature. nas 10.0.0.1 key shared_secret !--- Identifies
itself as a RADIUS server, reiterates !--- "localness"
and defines the key between the server (itself) and the
access point(itself). ! group testuser !--- Groups are
optional. ! user user1 nthash password1 group testuser
!--- Individual user user user2 nthash password2 group
testuser !--- Individual user !--- These individual
users comprise the Local Database ! radius-server host
10.0.0.1 auth-port 1812 acct-port 1813 key shared_secret
!--- Defines where the RADIUS server is and the key
between !--- the access point (itself) and the server.
radius-server retransmit 3 radius-server attribute 32
include-in-access-req format %h radius-server
authorization permit missing Service-Type radius-server
vsa send accounting bridge 1 route ip ! ! line con 0
line vty 5 15 ! end
```

配置客户端适配器

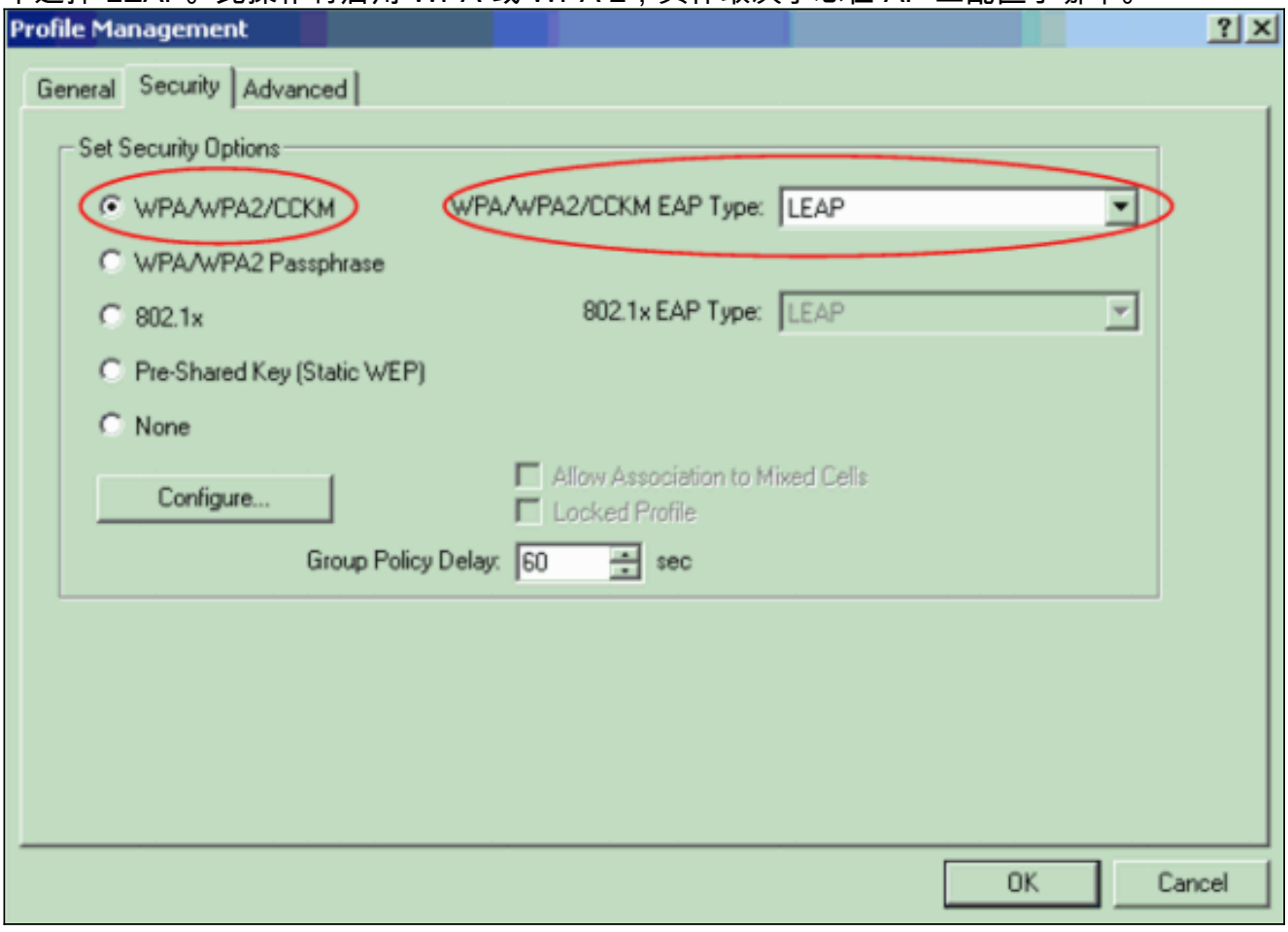
完成这些步骤：

注意： 本文档使用运行固件版本 2.5 的 Aironet 802.11a/b/g 客户端适配器，并介绍了如何使用 ADU 版本 2.5 配置客户端适配器。

1. 在 ADU 上的“Profile Management”窗口中，单击 **New** 以创建一个新配置文件。此时将显示一个新窗口，您在其中可以为 WPA 2 企业模式操作设置配置。在“General”选项卡下，输入客户端适配器将使用的配置文件名称和 SSID。在本示例中，配置文件名称和 SSID 均为 WPA2：**注意：** 该 SSID 必须与您在 AP 上为 WPA 2 配置的 SSID 匹配。

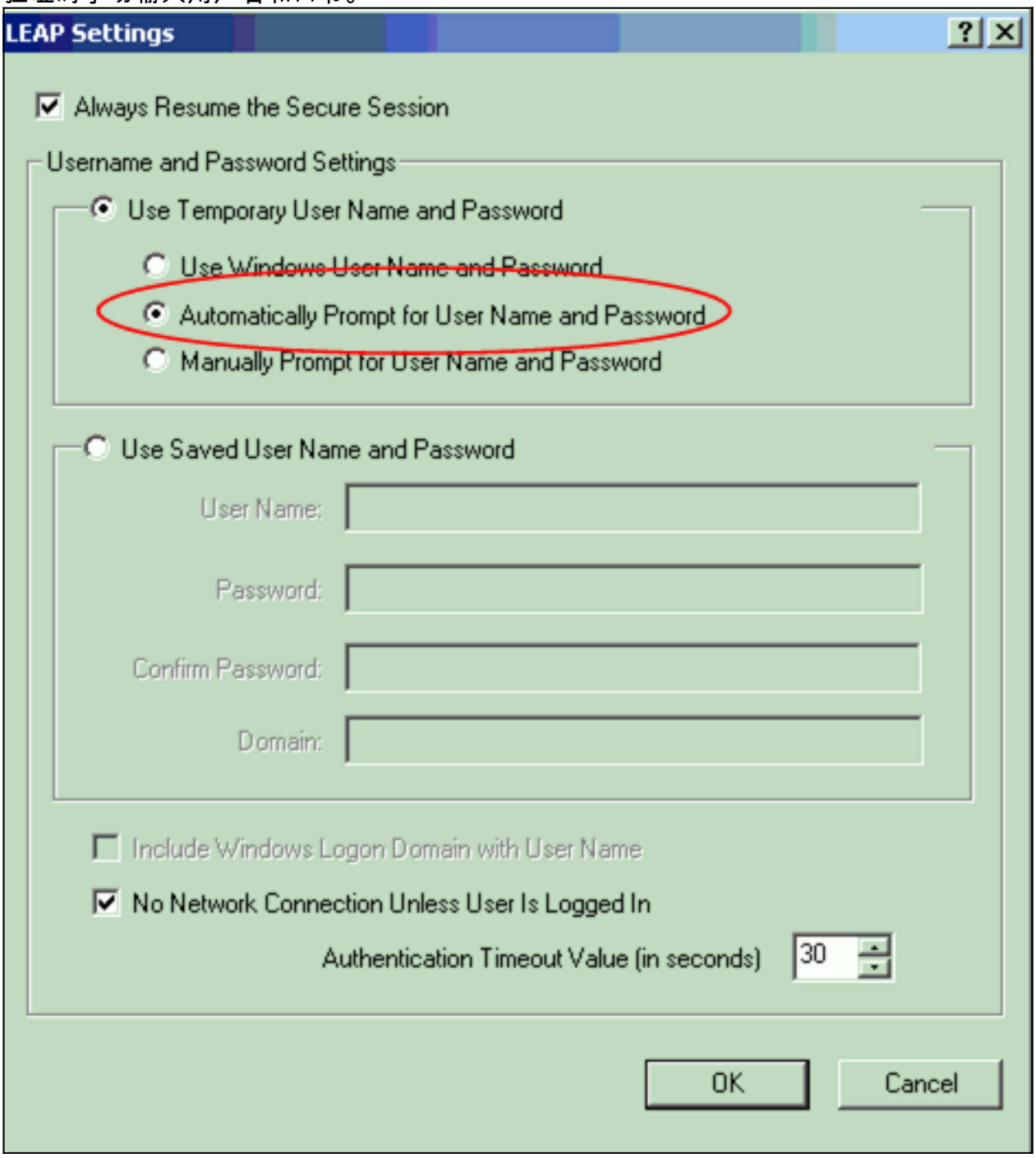


2. 单击 **Security** 选项卡，单击 WPA/WPA2/CCKM，然后从 WPA/WPA2/CCKM EAP Type 菜单中选择 LEAP。此操作将启用 WPA 或 WPA 2，具体取决于您在 AP 上配置了哪个。

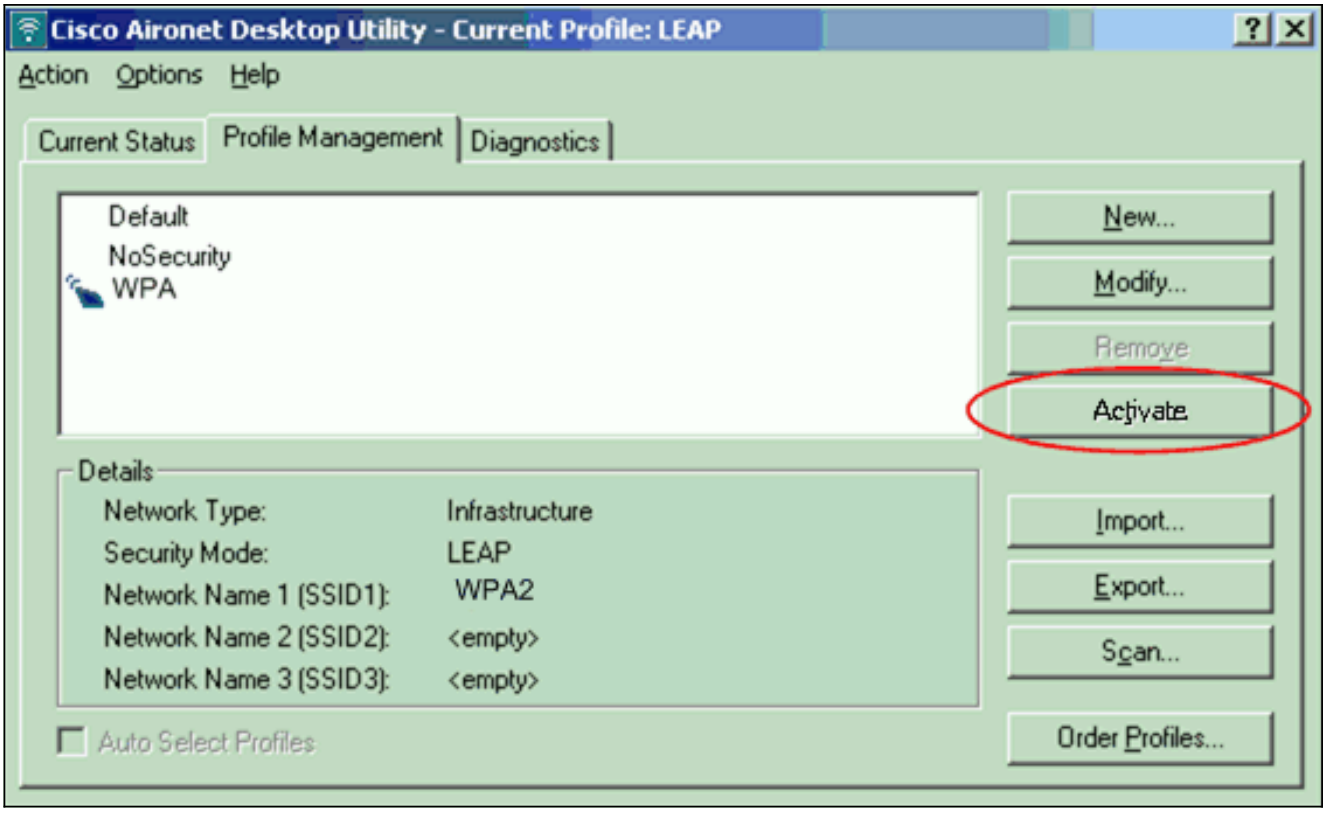


3. 单击 **Configure** 以定义 LEAP 设置。

4. 根据需要选择相应的 Username and Password Settings，然后单击 **OK**。此配置选择选项 Automatically Prompt for User Name and Password。通过选择此选项可以在进行 LEAP 身份验证时手动输入用户名和口令。



5. 单击 **OK** 以退出 Profile Management 窗口。
6. 单击 **Activate** 以在客户端适配器上启用此配置文件。

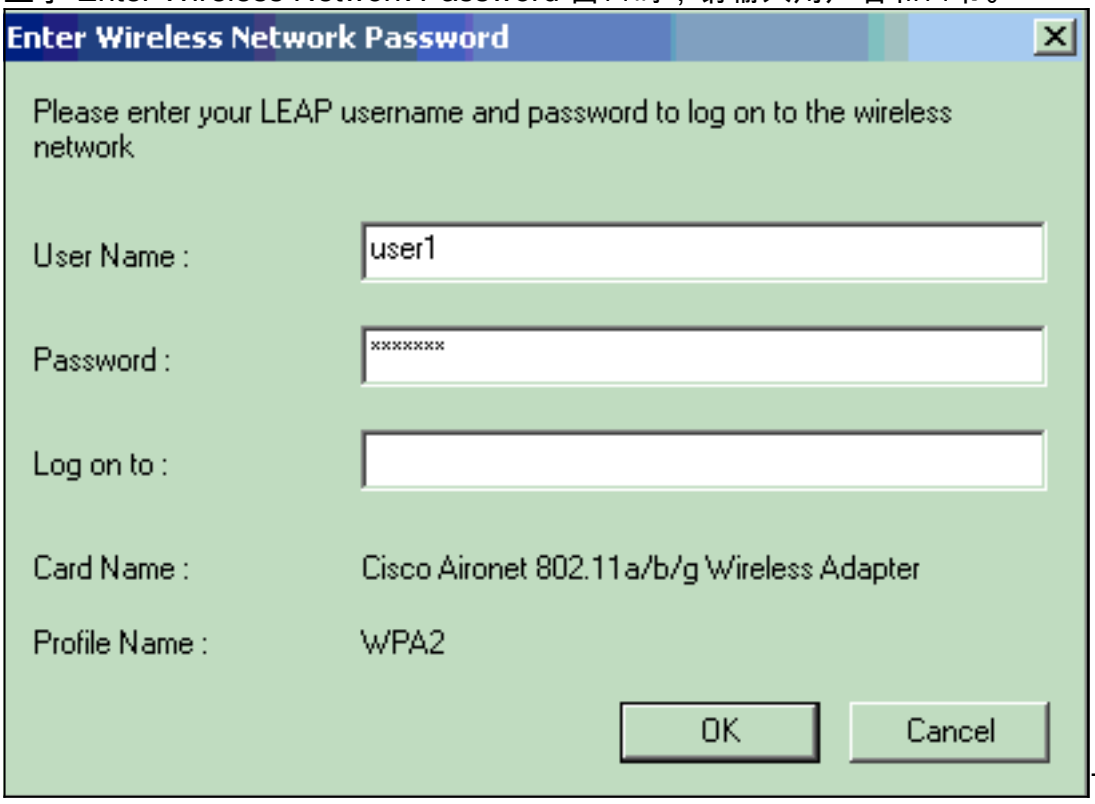


注意： 如果使用Microsoft无线零配置(WZC)配置客户端适配器，默认情况下， WPA2不是可用的与WZC。因此，要允许启用了 WZC 的客户端运行 WPA 2，必须安装 Microsoft Windows XP 的一个热修补程序。有关此安装的信息，请参阅 Microsoft 下载中心 - Windows XP 的更新 (KB893357) 。安装此热修补程序后，您将可以使用 WZC 配置 WPA 2。

验证

使用本部分可确认配置能否正常运行。

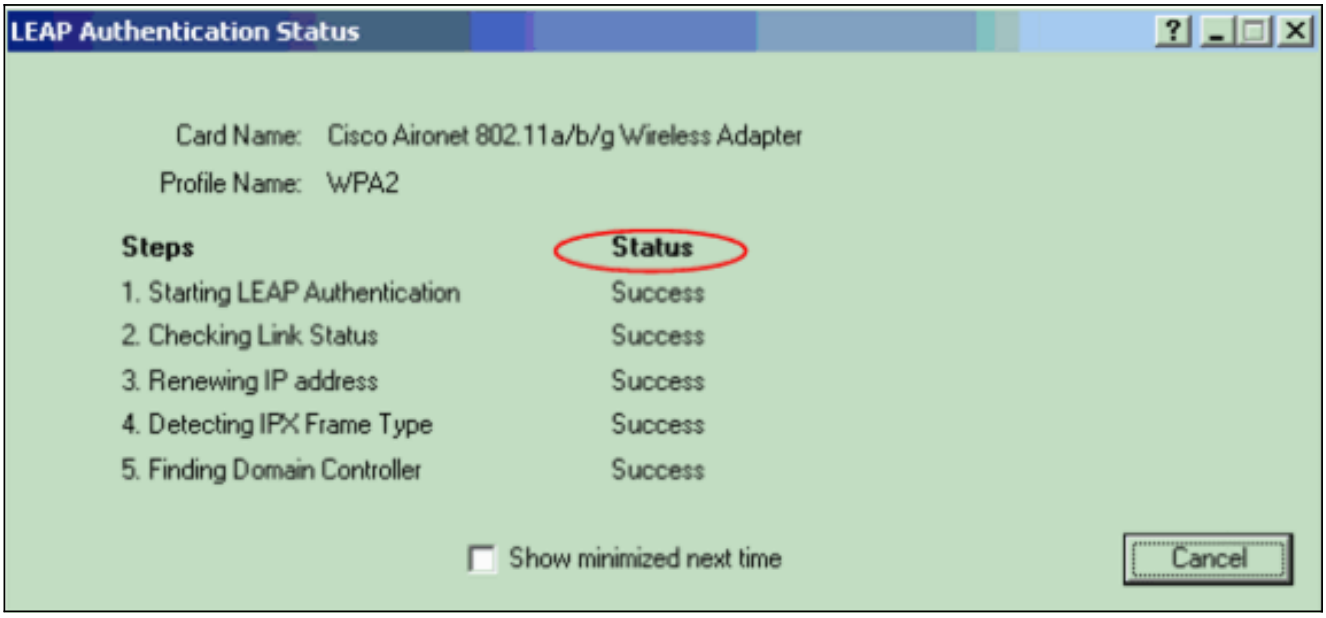
1. 显示 Enter Wireless Network Password 窗口时，请输入用户名和口令。



下一个窗口是

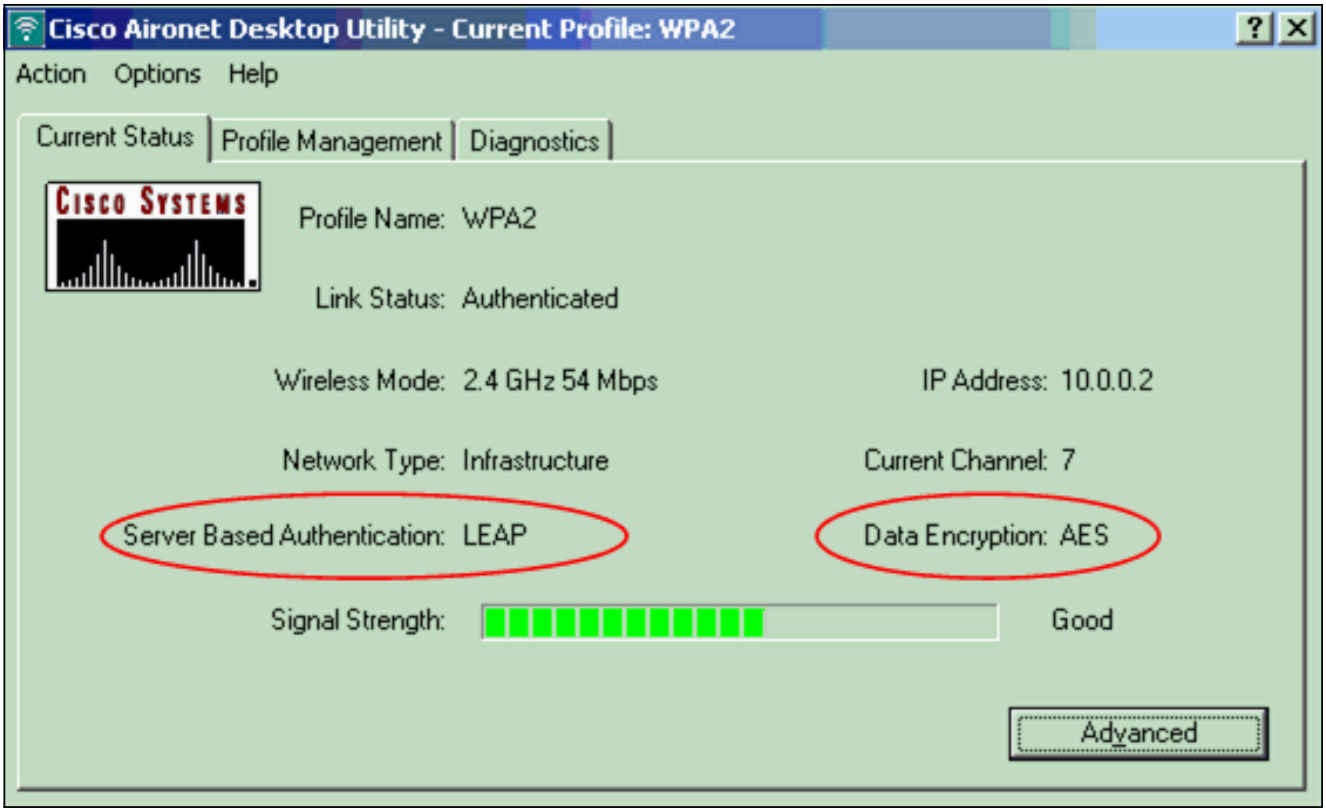
LEAP Authentication Status。此阶段将根据本地 RADIUS 服务器验证用户凭据。

2. 检查 Status 区域以查看身份验证的结果。



如果身份验证成功，客户端将连接到无线 LAN。

3. 检查 ADU Current Status 以验证客户端是否使用了 AES 加密和 LEAP 身份验证。这表示您已在 WLAN 中使用 LEAP 身份验证和 AES 加密实施了 WPA 2。



4. 检查 AP/bridge Event Log 以验证是否已成功使用 WPA 2 对客户端进行了身份验证。

故障排除

目前没有针对此配置的故障排除信息。

在个人模式下配置

术语**个人模式**是指经过测试，可以在仅 PSK 操作模式下互操作以进行身份验证的产品。此模式要求在 AP 和客户端上手动配置 PSK。PSK 在客户站和 AP 上都通过口令或标识码对用户进行身份验证。不需要任何身份验证服务器。仅当客户端口令与 AP 口令匹配时，该客户端才能获得对网络的访问权。口令还提供 TKIP 或 AES 用来生成加密密钥以对数据包进行加密的密钥材料。个人模式是针对 SOHO 环境的；对于企业环境，它被认为是不安全的。本部分提供在个人操作模式下实施 WPA 2 所需的配置。

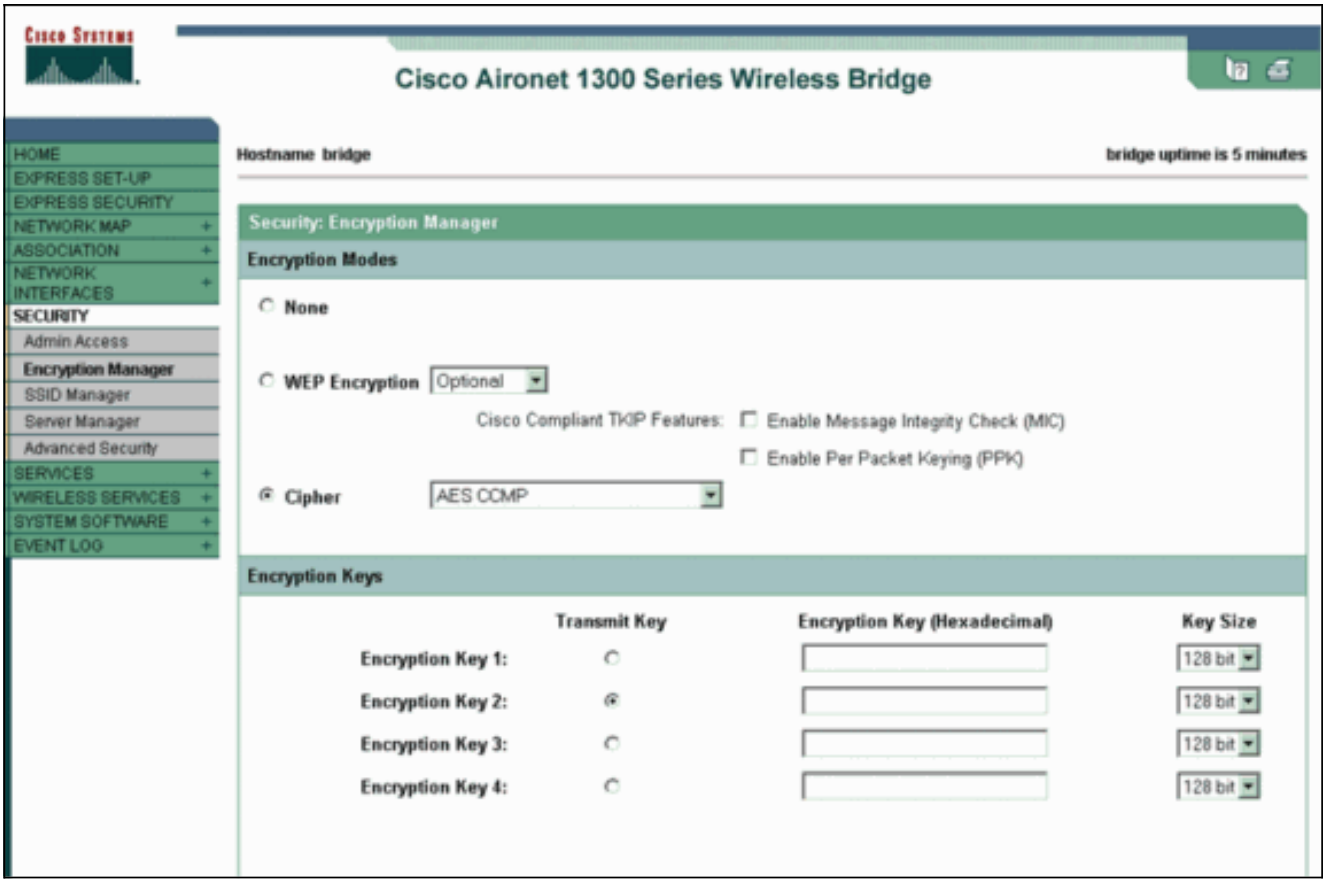
网络设置

在此设置中，使用与 WPA 2 兼容的客户端适配器的用户向 Aironet 1310G AP/网桥进行身份验证。在配置了 AES-CCMP 加密的情况下，使用 WPA 2 PSK 时会发生密钥管理。配置 AP 和配置客户端适配器部分显示了 AP 和客户端适配器上的配置。

配置 AP

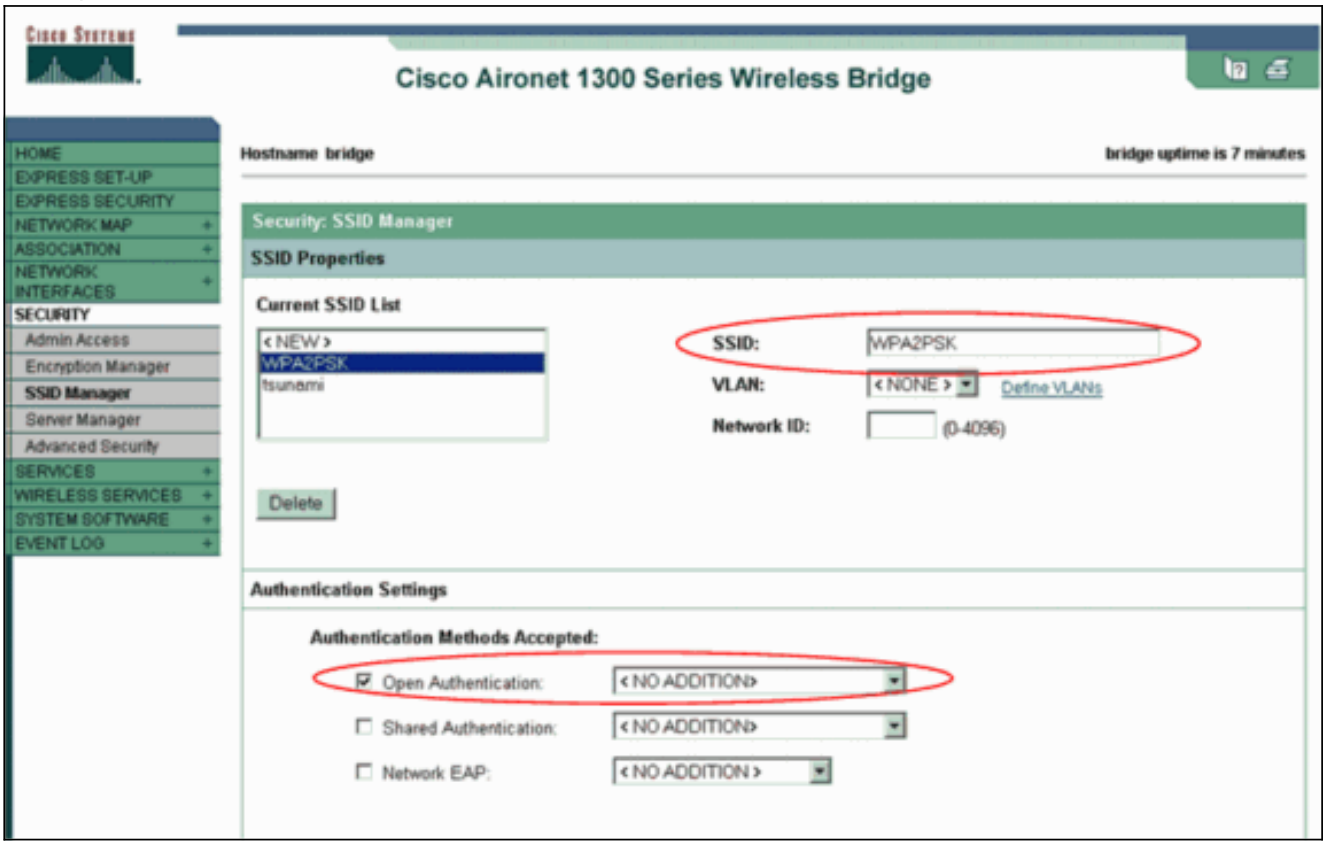
完成这些步骤：

1. 在左侧菜单中选择 **Security > Encryption Manager**，并完成以下步骤：在 Cipher 菜单中，选择 **AES CCMP**。此选项通过将计数器模式和 CCMP 结合使用来启用 AES 加密。

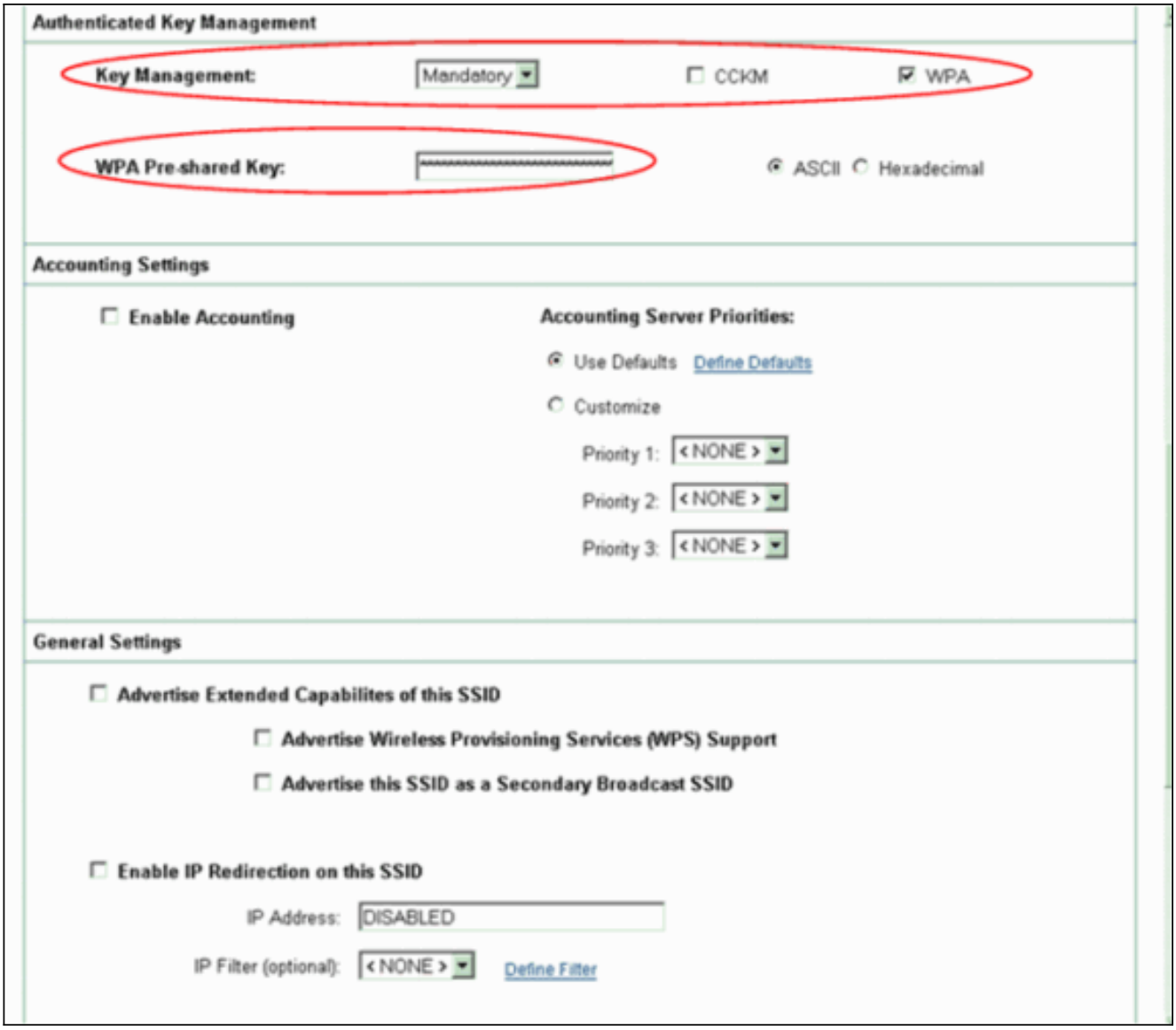


单击 **Apply**。

2. 选择 **Security > SSID Manager**，并创建用于 WPA 2 的新 SSID。选中 **Open Authentication** 复选框。



将 Security: SSID Manager 窗口向下滚动到 Authenticated Key Management 区域，并完成以下步骤：在 Key Management 菜单中，选择 **Mandatory**。选中右侧的 **WPA** 复选框。



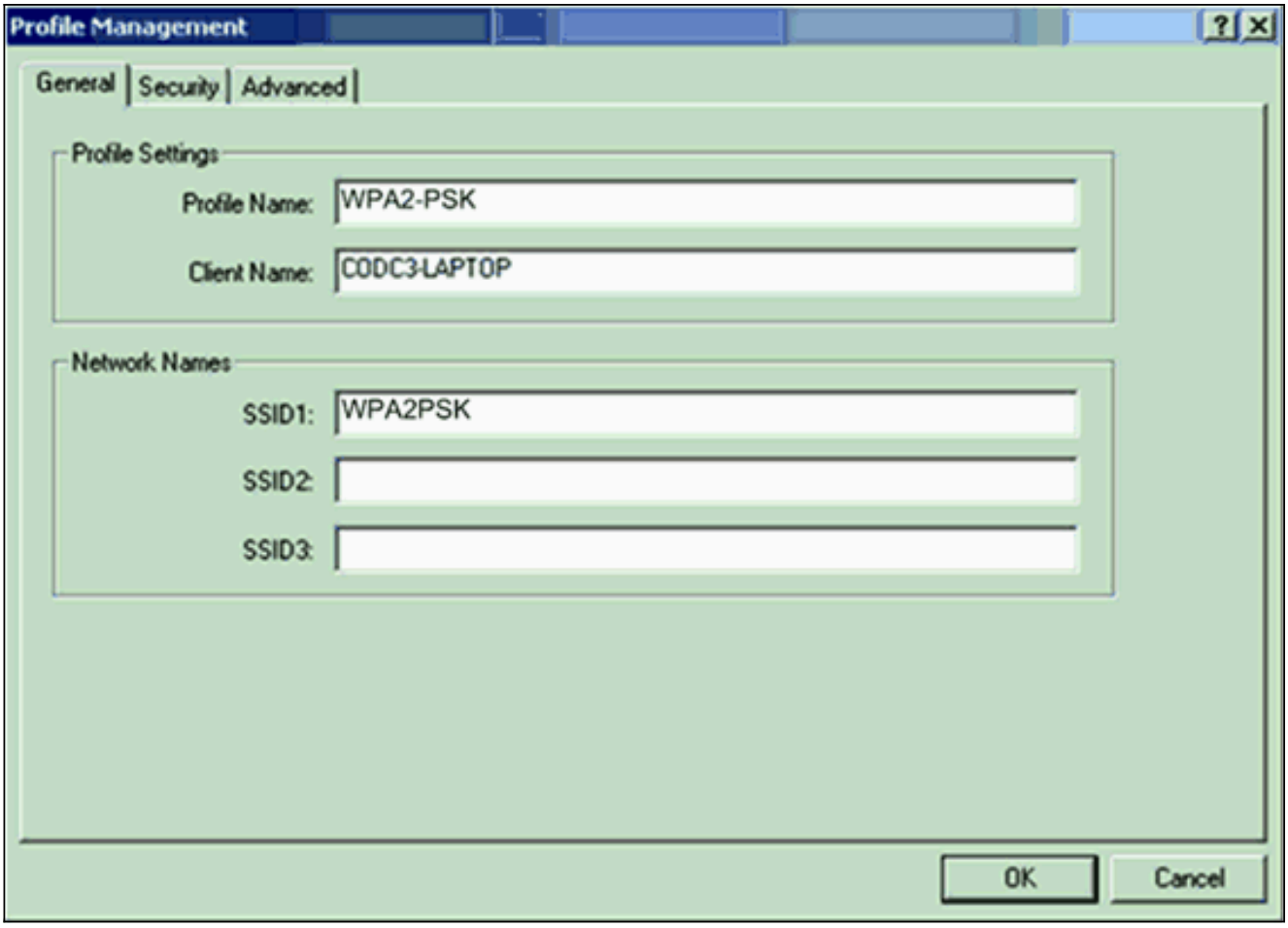
输入 WPA PSK 共享密钥或 WPA PSK 密码短语密钥。该密钥必须与您在客户端适配器上配置的 WPA PSK 密钥匹配。单击 **Apply**。

AP 可以立即接收来自无线客户端的身份验证请求。

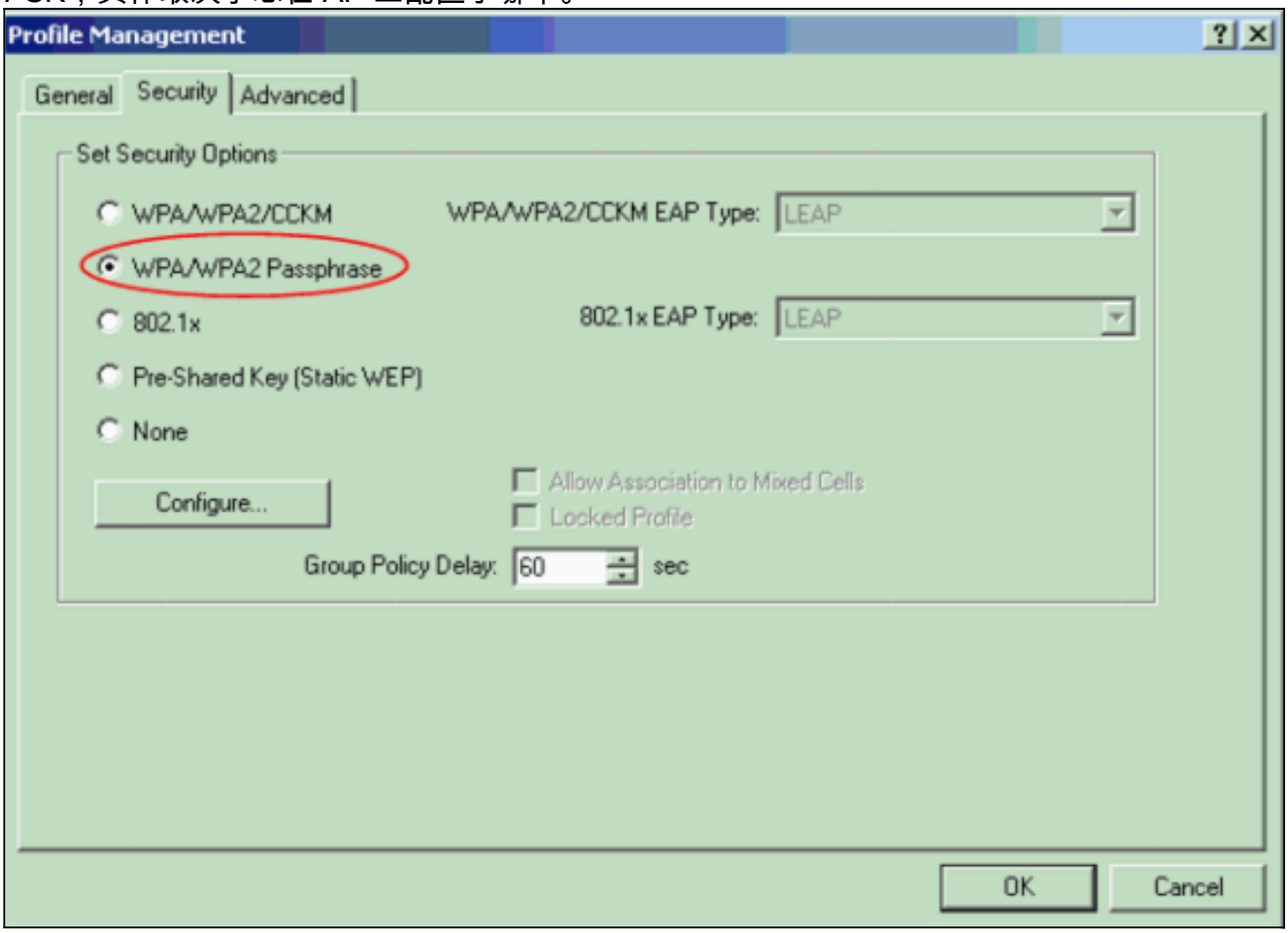
配置客户端适配器

完成这些步骤：

1. 在 ADU 上的“Profile Management”窗口中，单击 **New** 以创建一个新配置文件。此时将显示一个新窗口，您可以在其中为 WPA 2 PSK 操作模式设置配置。在“General”选项卡下，输入客户端适配器将使用的配置文件名称和 SSID。在本示例中，配置文件名称为 WPA2-PSK，且 SSID 为 WPA2PSK：**注意：** 该 SSID 必须与您在 AP 上为 WPA 2 PSK 配置的 SSID 匹配。

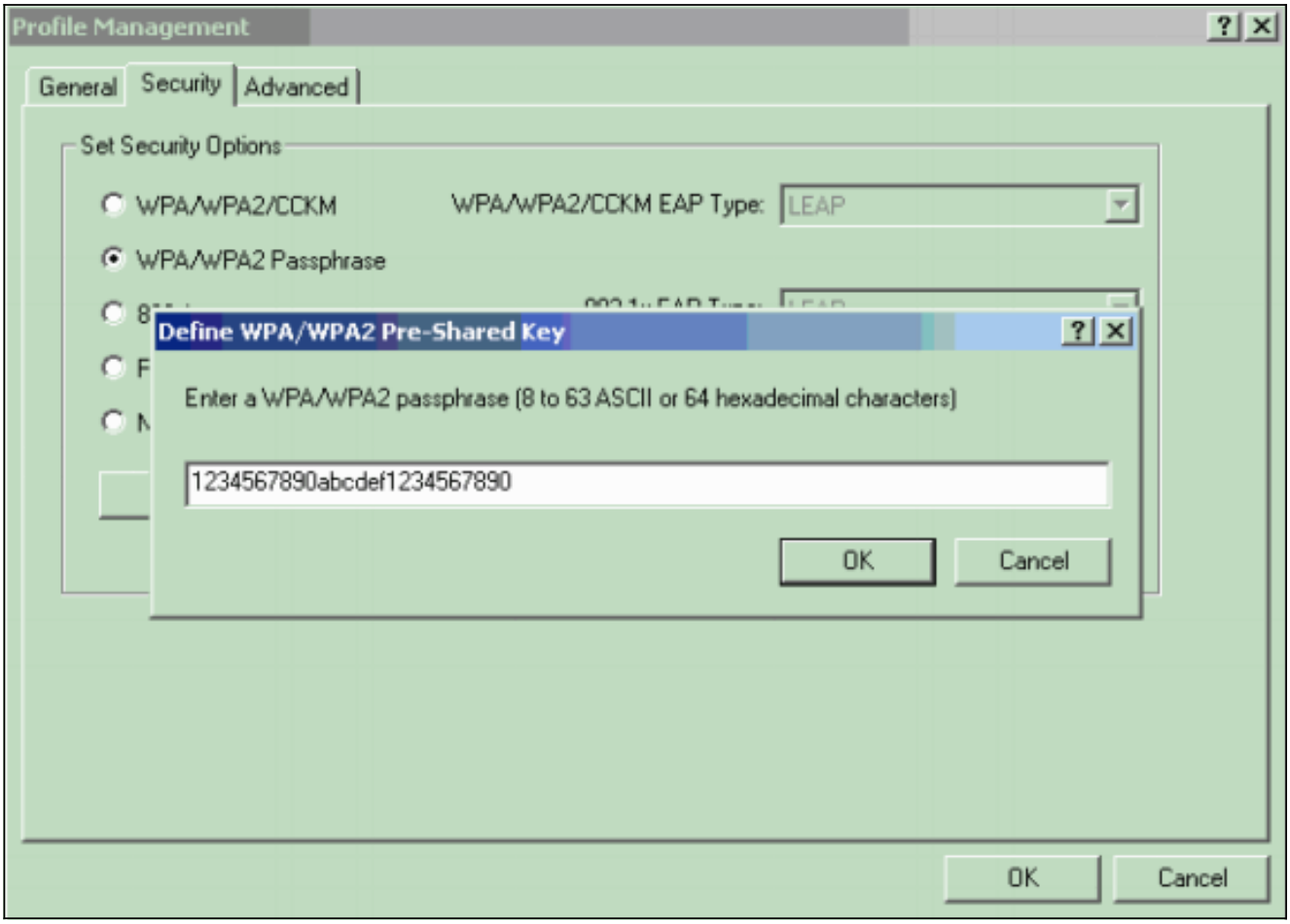


2. 单击 **Security** 选项卡，并单击 WPA/WPA2 Passphrase。此操作将启用 WPA PSK 或 WPA 2 PSK，具体取决于您在 AP 上配置了哪个。



3. 单击 **Configure**。此时将显示 Define WPA/WPA2 Pre-Shared Key 窗口。

4. 从系统管理员处获得 WPA/WPA2 密码短语，然后在 WPA/WPA2 passphrase 字段中输入该密码短语。获得基础架构网络中 AP 的密码短语或对等网络中其他客户端的密码短语。请使用以下准则输入密码短语：WPA/WPA2 密码短语必须包含 8 到 63 个之间的 ASCII 文本字符或 64 个十六进制字符。您的客户端适配器 WPA/WPA2 密码短语必须和您计划与其通信的 AP 的密码短语匹配。



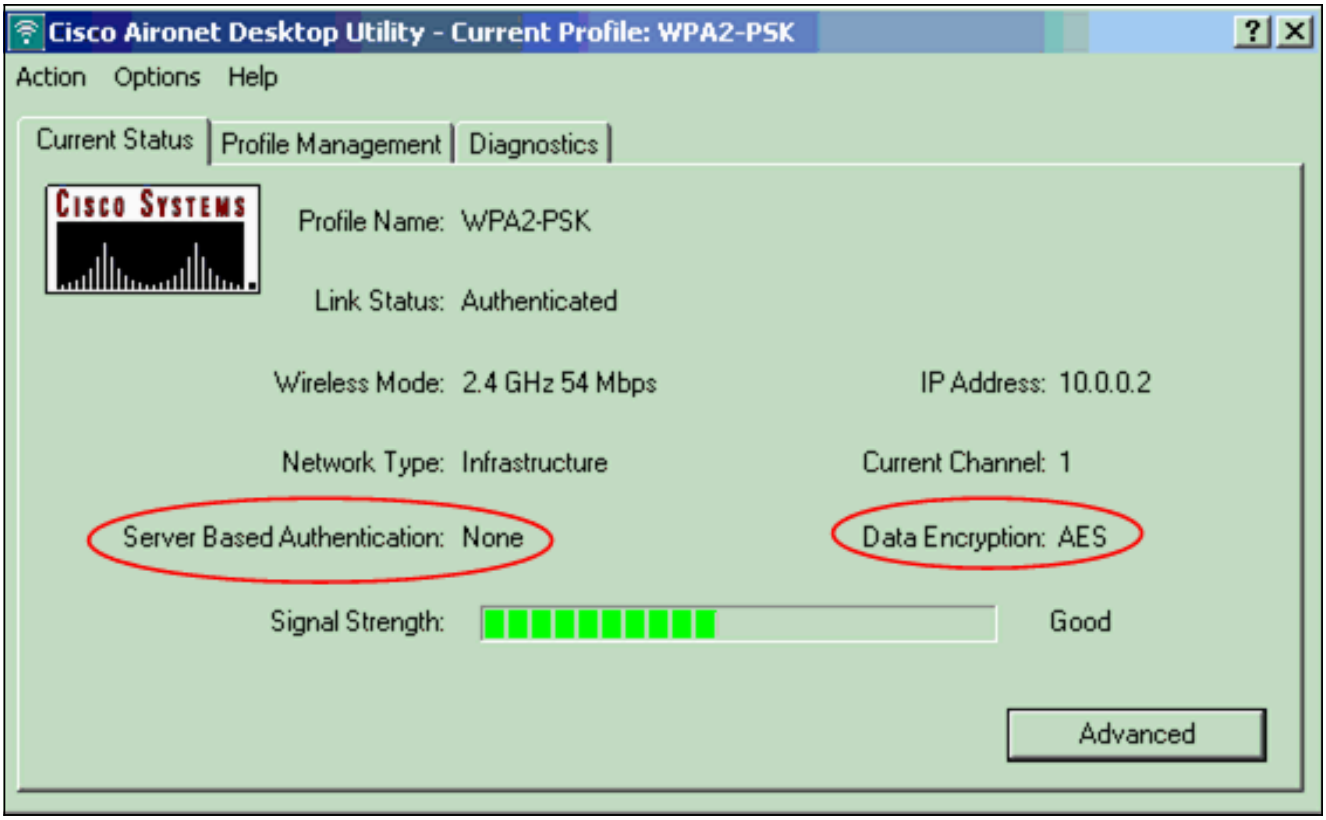
5. 单击 **OK** 以保存密码短语并返回到 Profile Management 窗口。

验证

使用本部分可确认配置能否正常运行。

在WPA2 PSK配置文件激活后， AP验证根据WPA2密码短语(PSK)和对WLAN的提供访问的客户端。

1. 检查 ADU Current Status 以验证身份验证是否成功。此窗口提供了一个示例。此窗口显示所使用的加密为 AES，并且未执行任何基于服务器的身份验证
：



2. 检查 AP/bridge Event Log 以验证是否已成功使用 WPA 2 PSK 身份验证模式对客户端进行了身份验证。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 配置密码套件和 WEP
- 配置身份验证类型

- WPA 配置概述
- WPA2 -Wi-Fi 安全访问 2, Wi-Fi 安全访问 2
- 什么是WPA混合模式的操作，并且我如何在我的AP配置它
- 无线支持页
- 技术支持和文档 - Cisco Systems