WPA2配置范例

介绍

本文介绍在 WLAN（无线网络）中使用 WPA2（Wi-Fi 访问保护 2）的优点。在文件中将通过提供两个配置范例，介绍怎样在无线网络中完善 WPA2，第一个范例说明怎样在企业模式配置 WPA2，第二个范例说明在个人模式配置。

【译者注】WPA 使用可扩展的认证协议（EAP）

配置条件

必要条件

在配置前，请先确定掌握以下知识点：

（1） WPA

（2） 无线安全解决方案

注释：涉及无线胖 AP 安全解决方案，请参考以下网址

http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/ps4076/prod_brochure09186a00801f7d0b.html

使用说明

本文涉及的内容基于以下软件及硬件版本：

（1） 使用 12.3（2）JA 软件版本的思科 1310G AP/Bridge

（2） 使用固件 2.5 的思科 802.11a/b/g CB21AG 客户端

（3） 使用固件 2.5 的思科桌面软件（Aironet Desktop Utility）

【译者注】客户端 CB21AG 和 PI21AG 软件与其它客户端使用软件不同，必须使用 Aironet Desktop Utility（ADU）与 CB21AG 或 PI21AG 网卡配合使用，使用 Aironet Client Utility (ACU)与其它客户端配合使用.更多关于安装 ADU 与 CB21AG 客户端信息，请参考以下网址：

http://www.cisco.com/en/US/docs/wireless/wlan_adapter/cb21ag/user/1.0/configuration/guide/winch3kh.html

此文档中涉及的 AP 都是使用内置天线，如果使用外置天线，请先检查天线是否和 AP 连接，否则，AP 不能连接无线网络。某些型号的 AP 已经内置天线，但有些需要配置外置天线使用。对于不同型号 AP 的详细描述，请参考产品手册。

本文中所描述的所有内容在实验室环境实现，所有设备都是初始配置。在真实环境中，请先确定各命令的意义，再做配置。

规定

请参考以下网址，获得更多信息
http://www.cisco.com/en/US/tech/tk801/tk36/technologies_tech_note09186a0080121ac5.shtml

知识点

WPA 是 Wi-Fi 联盟提出的一种标准的无线网络(Wi-Fi)安全的系统，它是应研究者在前一代的系统有线等效加密（WEP）中找到的几个严重的弱点而产生的。WPA 实现了 IEEE 802.11i 标准的大部分，是在 802.11i 完备之前替代 WEP 的过渡方案。它提供增强的数据保护以及访问控制，为企业、办公室以及 SOHO 环境提供更安全的解决方案。

WPA2 是下一代的无线网络安全技术，WPA2 现在隶属于被 IEEE 认可的 IEEE 802.11i 安全标准，WPA2 基于 AES(Advancde EncryptionStandard) 加密算法和 CCM(Counter - Mode) 认证方式，AES 标准支持对数据包进行 128 位的加密。CCMP 算法生成一个 MIC 对无线网络上数据提供初始认证及完整性检查。

【译者注】相比 WPA 使用 TKIP 加密，WPA2 使用的 AES 加密，为数据提供更安全的加密方法，WPA2 为每一个链接建立会话链接，为每一个客户使用唯一的加密密钥.这样，每个数据包在传输中使用唯一的密钥。而且传输完成密钥不再使用.提供了增强的安全性。WPA 仍然是比较安全的，没有被破解的认证方式，但是思科建议使用 WPA2 来代替 WPA。

请参考以下网址获得对 WPA，WPA2 以及 802.11i 的更多信息。
http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008054339e.shtml
http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008054339e.shtml

WPA 和 WPA2 都支持以下模式：
（1） 企业模式
（2） 个人模式
本文档将完整描述 WPA2 在以上两个模式下的工作.

支持 WPA2 的思科设备

（1）1130AG,1230AG
（2）1100 系列
（3）1200 系列
（4）1300 系列

【译者注】以上设备都运行在 IOS12.3（2）JA 或者以上版本，利用 802.11g 频段

以下设备同样支持 WPA2 的 AES 加密
（1） 使用模块 AIR-RM21A 和 AIR-RM22A 的 1200 系列
【译者注】使用 AIR-RM20A 的 1200 系列不支持 WPA2

（2） 固件 2.5 的 802.11a/b/g 的客户端

【译者注】思科 350 系列不支持 WPA2，因其 Radio 不支持 AES。1400 系列不支持 WPA2 和 AES 加密。

企业模式配置

在企业模式下,可同时配置支持 PSK 和 802.11x 的认证，802.11x 因其多样、弹性的认证机制和强大的加密算法提供了较高的安全认证方式。在企业模式下的 WPA2 认证过程分为两步，第一阶段配置开放认证，第二阶段使用 802.1x 的 EAP 类型做认证，AES 提供加密。

在企业模式，客户端和认证服务器通过 EAP 认证方式相互认证，并产生一对主密钥（PMK），通过使用 WPA2，服务器会动态的产生 PMK 并传递给 AP。

本部分将讨论配置 WPA2 的必要部分。

网络设置

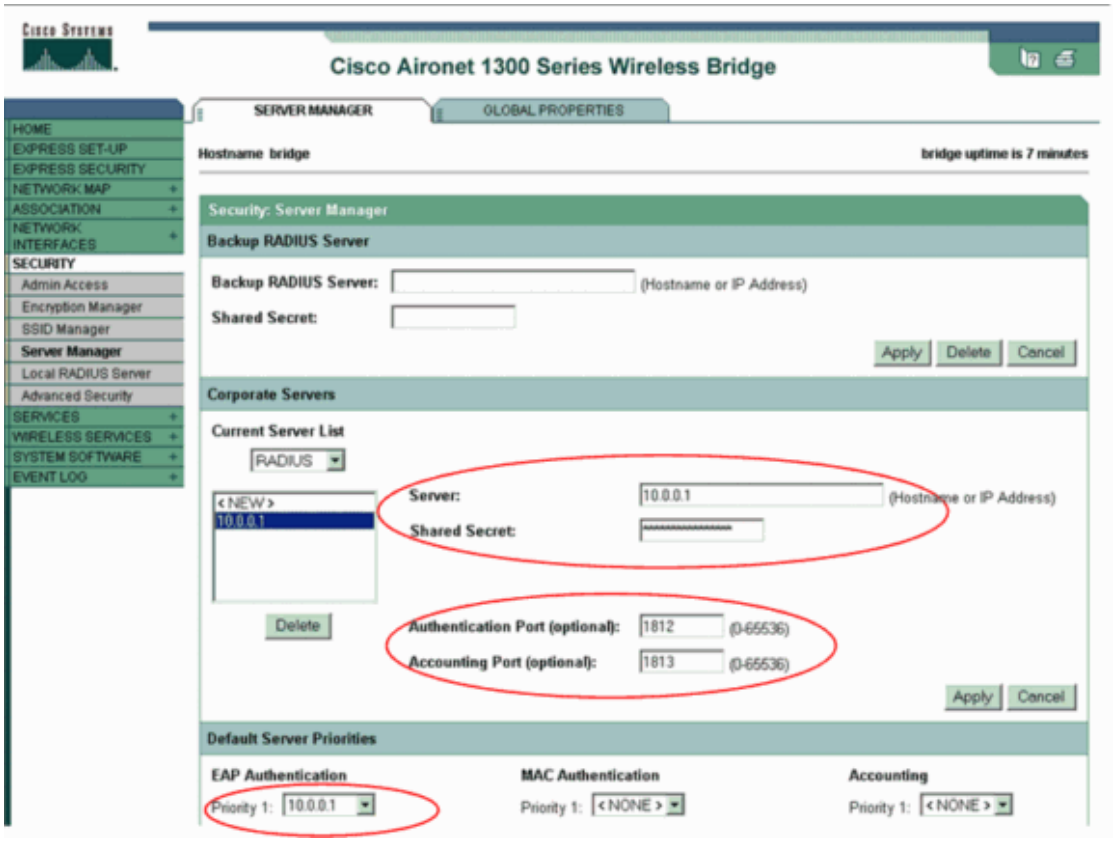
一个 1310AG 的 AP 会通过 LEAP 认证一个 WPA2 的客户端，通过配置 AES-CCMP 的加密方式提供 WPA2 的密钥管理，AP 被配置为本地的 LEAP 认证服务器。以下是配置过程。

配置 AP

1. 配置 AP 使用 LEAP 作为认证的本地认证服务器。

   A，选择 Security > Server Manager 配置本地认证服务器，定义 IP 地址，端口和 RADIUS 共享密码。

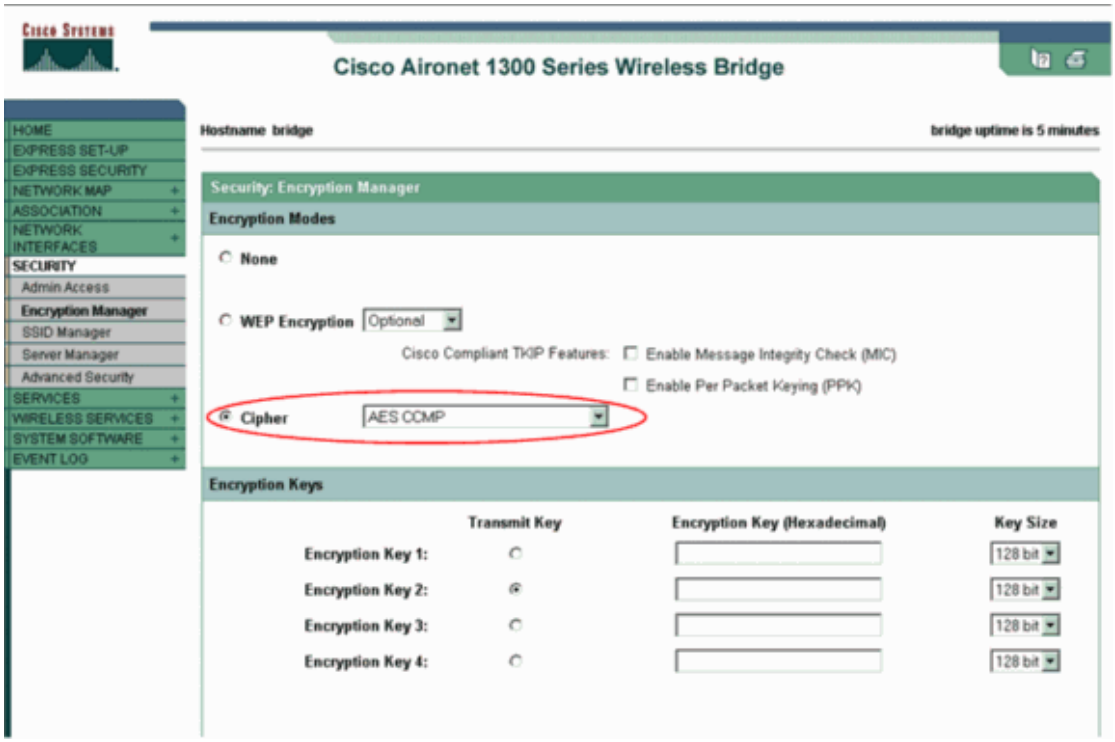
B，在 Defaul Server Priorities 区域，定义 EAP 认证优先级 10.0.0.1，它是本地的认证服务器。



2. 选择 Security > Encryption Manager

   A. 在 Cipher 栏，选择 AES CCMP

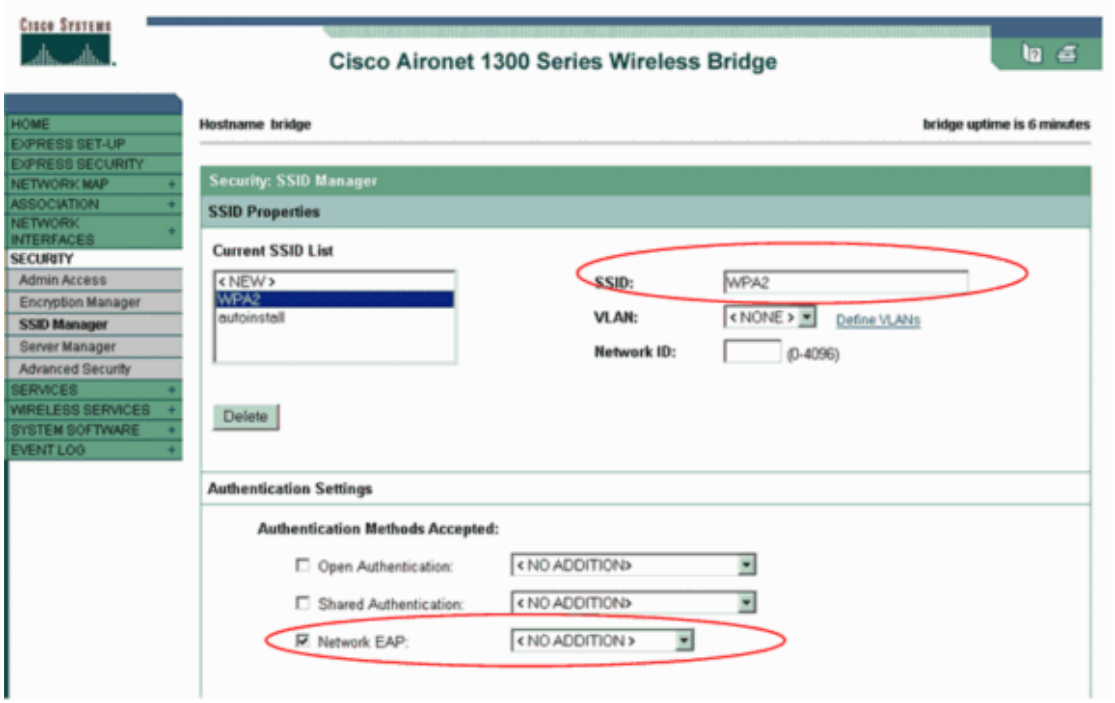
   这个选项打开 AES 加密



B. Apply

3. 选择 Security > SSID Manager 配置 SSID

A. 检查 Network EAP 的选项



【译者注】当在射频接口配置认证方式时，请参考以下指导：

（1） 思科客户端：使用网络 EAP.

（2） 第三方客户端（包括符合思科 CCX 的客户端）：使用开放的 EAP

（3） 思科和第三方客户端的组合：选择网络 EAP 和开放的 EAP

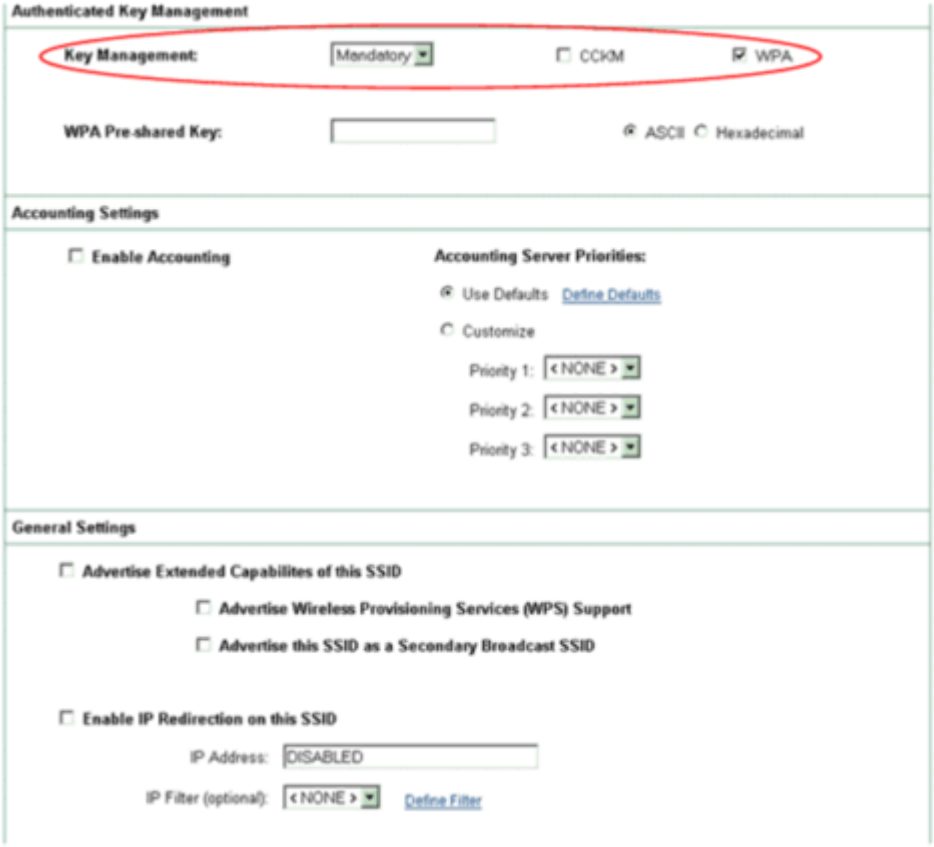
B. 下拉页面到认证密钥管理区域

a. 选择 **Mandatory**.

b. 检查 WPA

C. **Apply**.

【译者注】定义 VLAN 是可选的，如果定义了 VLAN，与此 SSID 相关联的客户端会进入 VLAN 中。



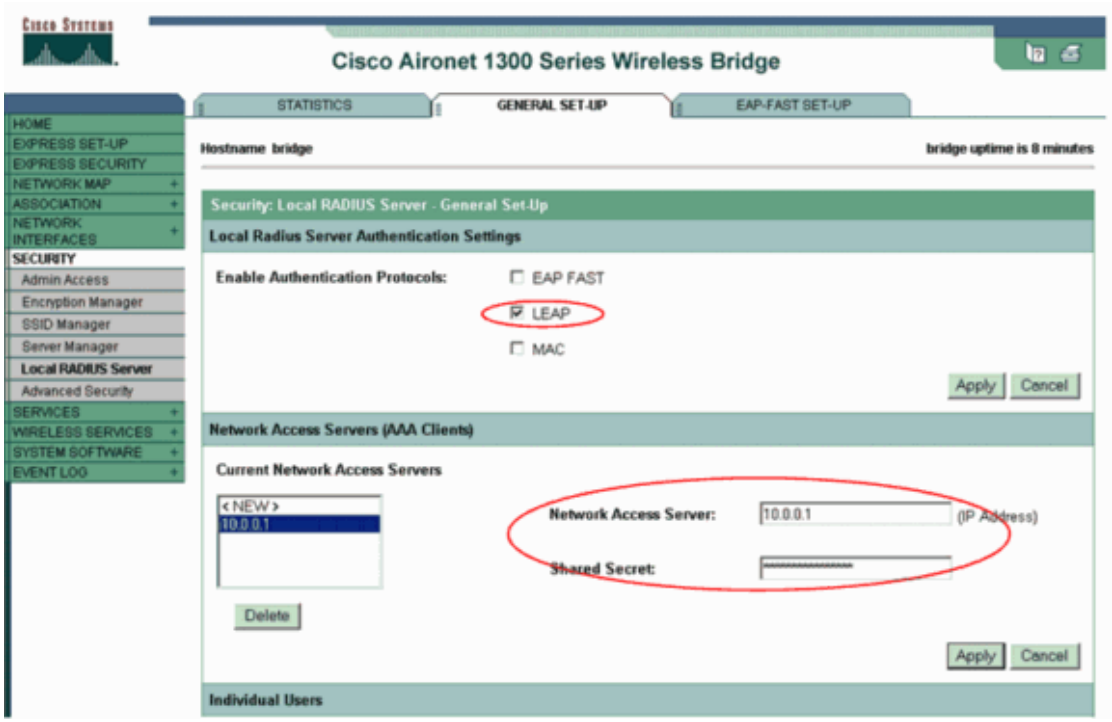
4. 选择 **Security > Local Radius Server**

A. 点击 General Set-Up

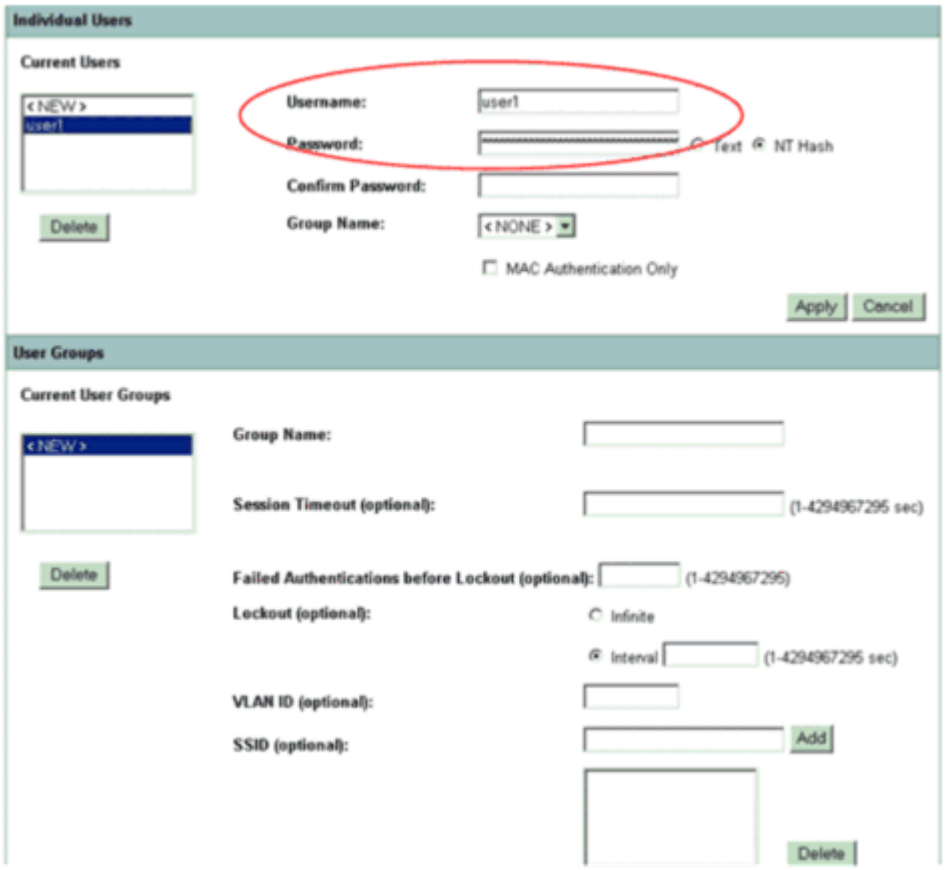
B. 选择 LEAP 然后 Apply

C. 在网络认证服务器上，定义 RADIUS 的 IP 地址和共享密码。
对于本地的 RADIUS 服务器，采用 AP 的 IP 地址。

D. Apply



5. 下拉页面到 Individual User 区域定义用户名称。用户组可选



以上配置定义了一个名为 user1 的用户，完成以上配置过程。AP 已经准备好接受客户端的认证请求，下面将配置客户端。

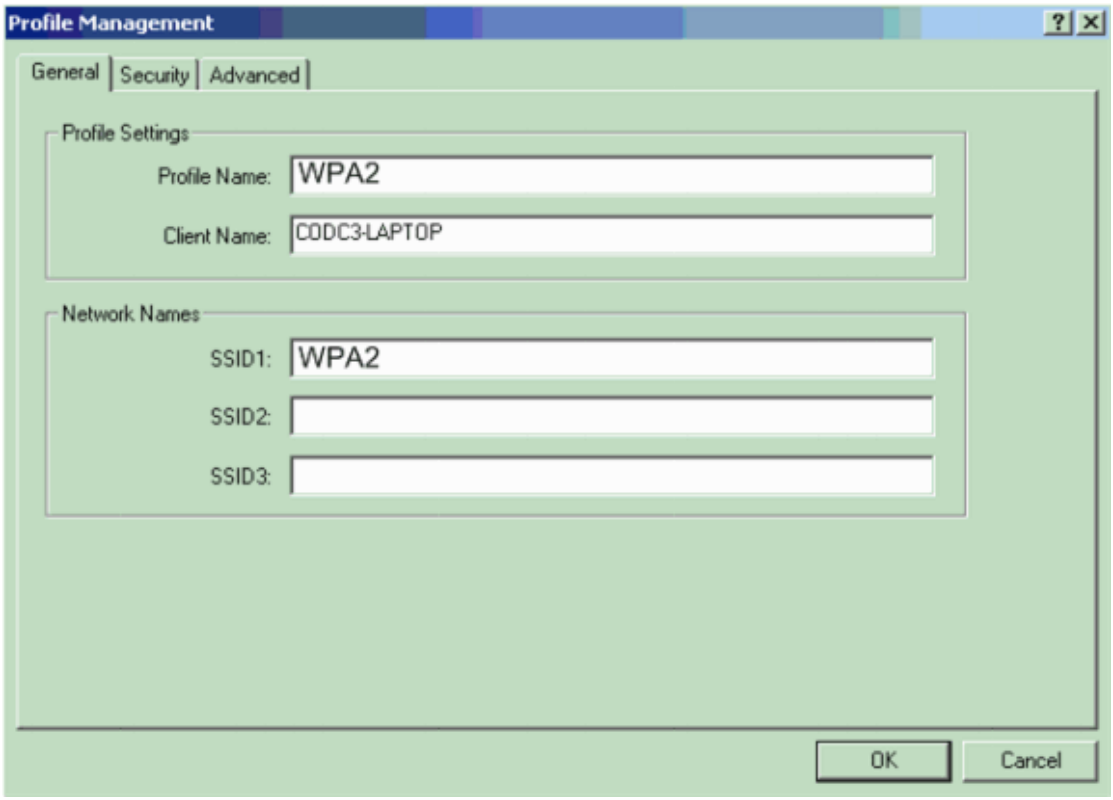
配置客户端

【译者注】此配置文档使用固件 2.5 的 802.11a/b/g 客户端，其配置使用 ADU2.5

1. 在 ADU 的帐户管理下，选择 new

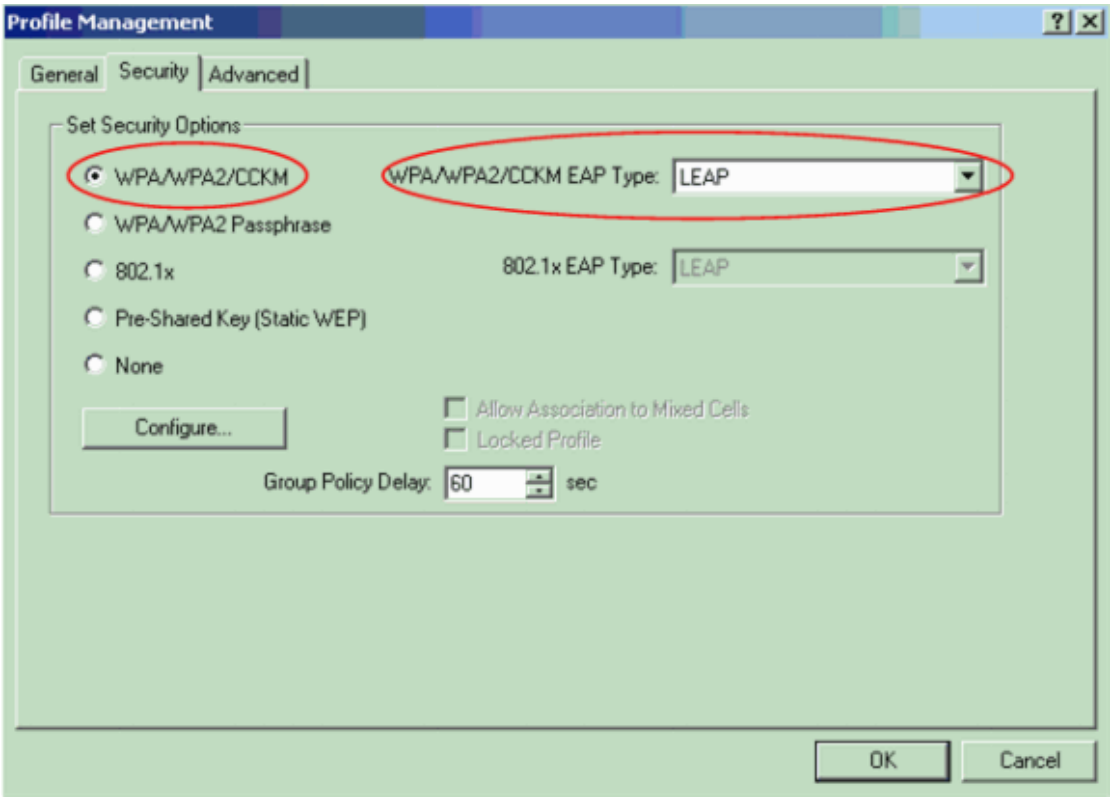
新窗口出现，在 General 部分，可以配置 SSID，WPA2 以及企业模式。

在此例中，Profile 名字和 SSID 均配置为 WPA2.(SSID 必需与运行 WPA2 的 AP 一致)

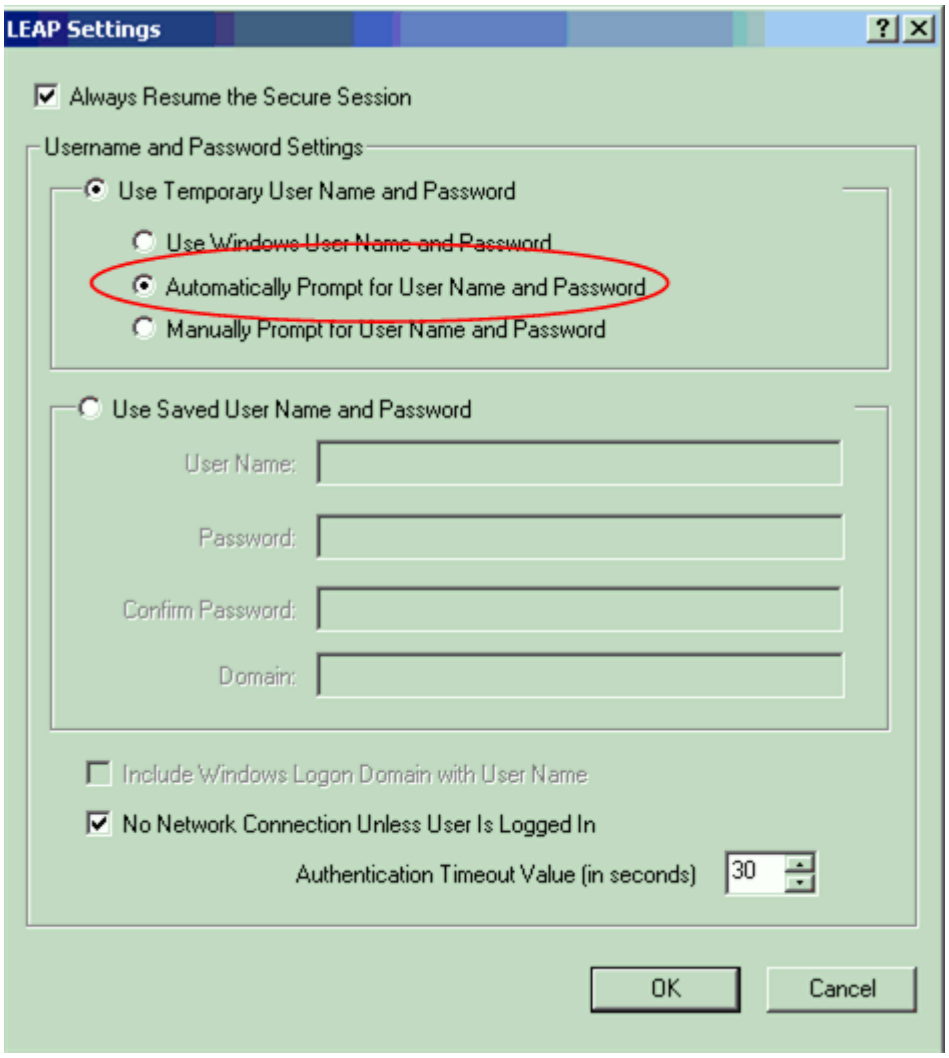


2. 选择 Security，点击 WPA/WPA2/CCKM，选择 LEAP

这个配置打开 WPA 或 WPA2

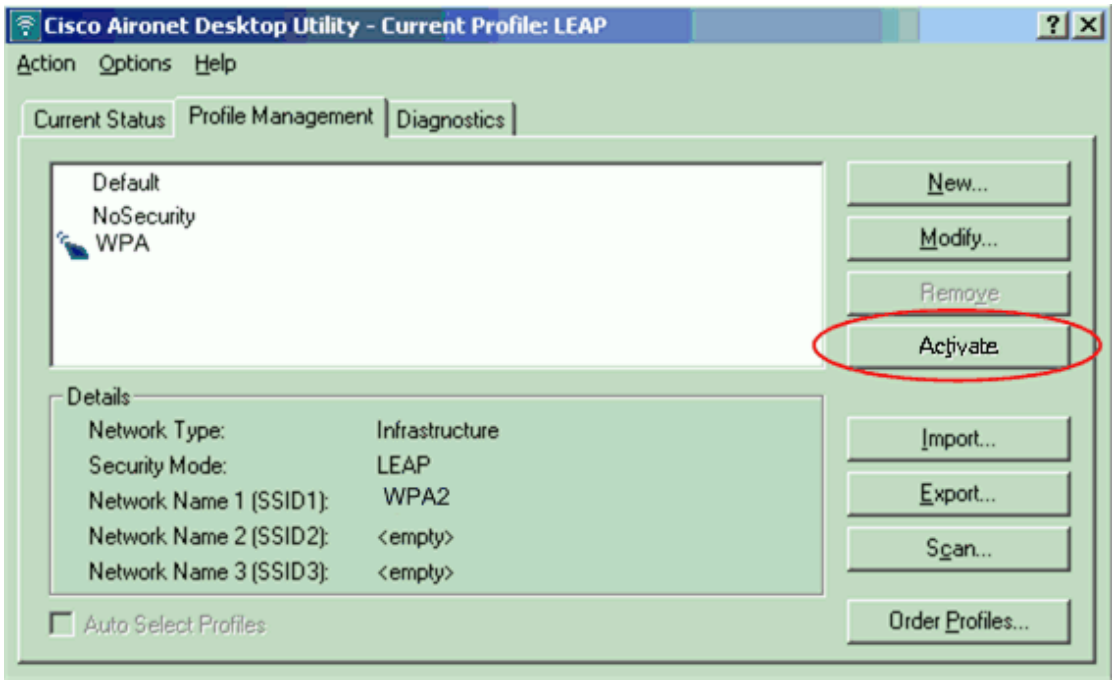


3. 选择 Configure 配置 LEAP 的设置
4. 选择用户名密码设置.
   这个例子中选择 Automatically Prompt for User Name and Passord.



5. 点击 OK

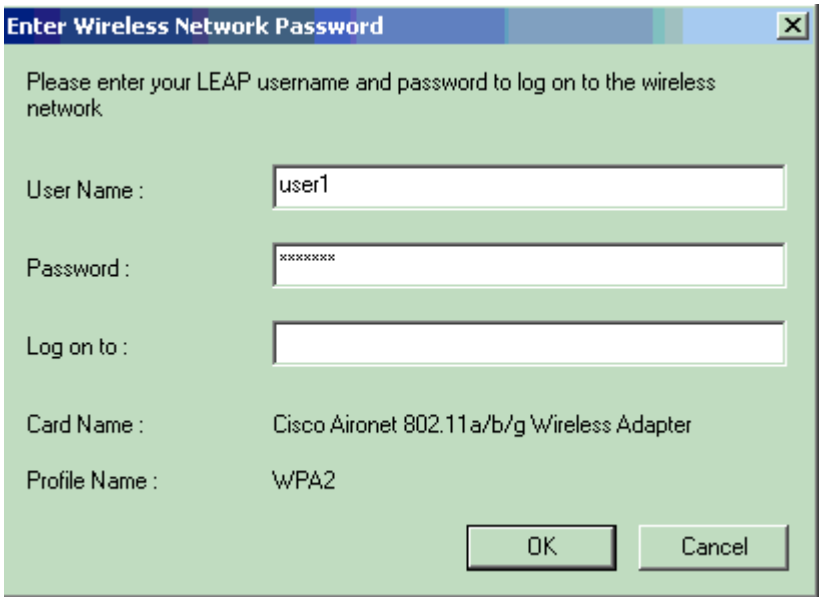
6. 点击 Activate 在客户端



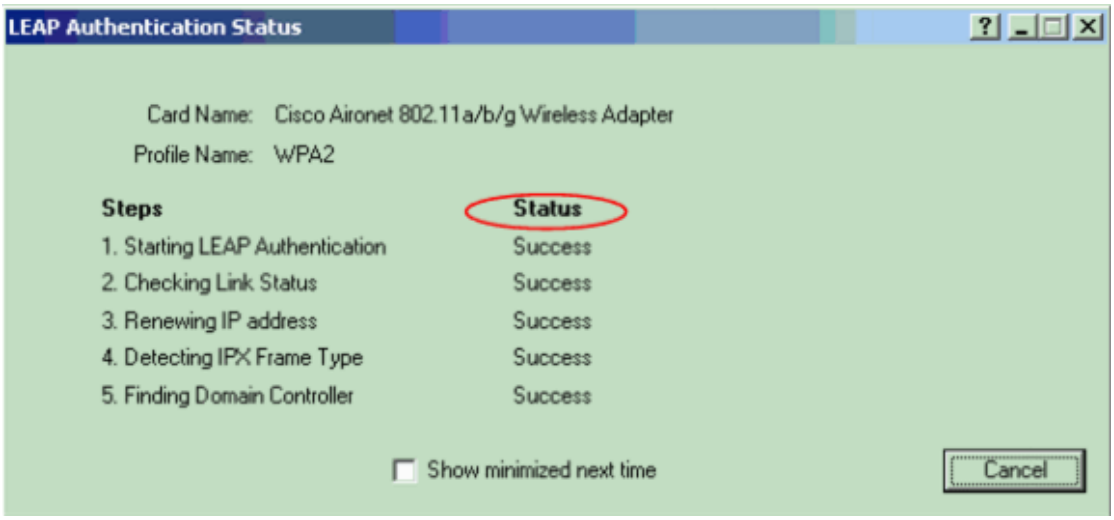
【译者注】如果使用微软的配置向导 WZC，默认下不支持 WPA2，请到以下网址，下载相应补丁 ，
http://www.microsoft.com/downloads/details.aspx?FamilyID=662BB74D-E7C1-48D6-95EE-1459234F4483&displaylang=en&Hash=NKWJBG4
升级补丁（KB893357）后，可采用 WZC 配置 WPA2.

验证

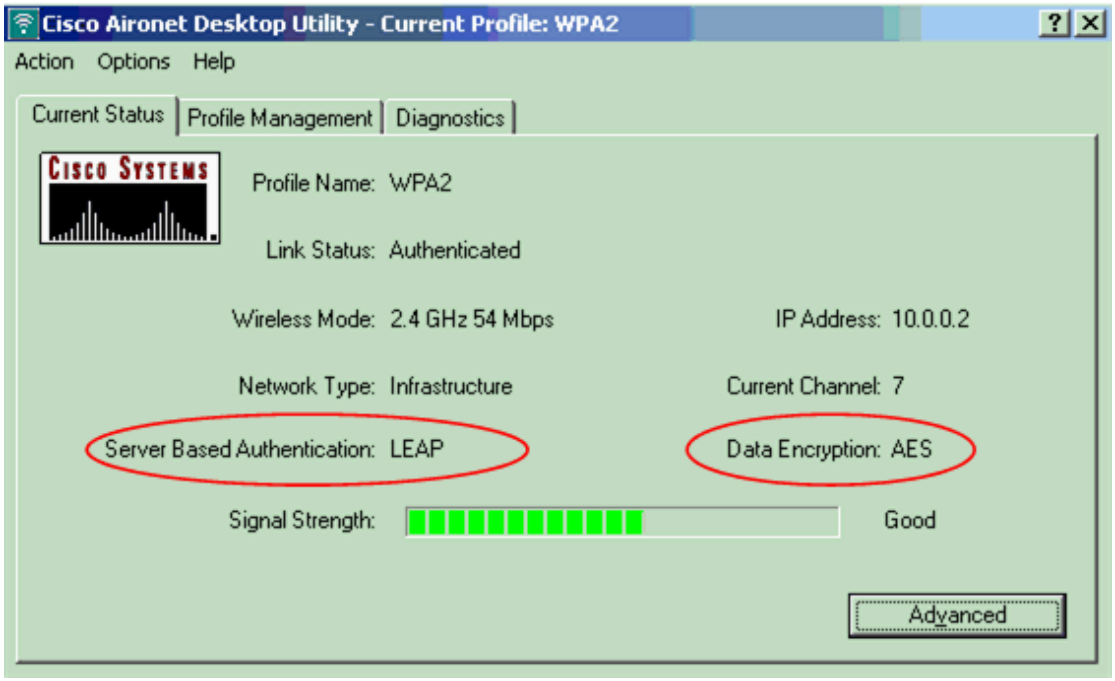
使用以下向导，检测配置情况
1. 输入用户名密码



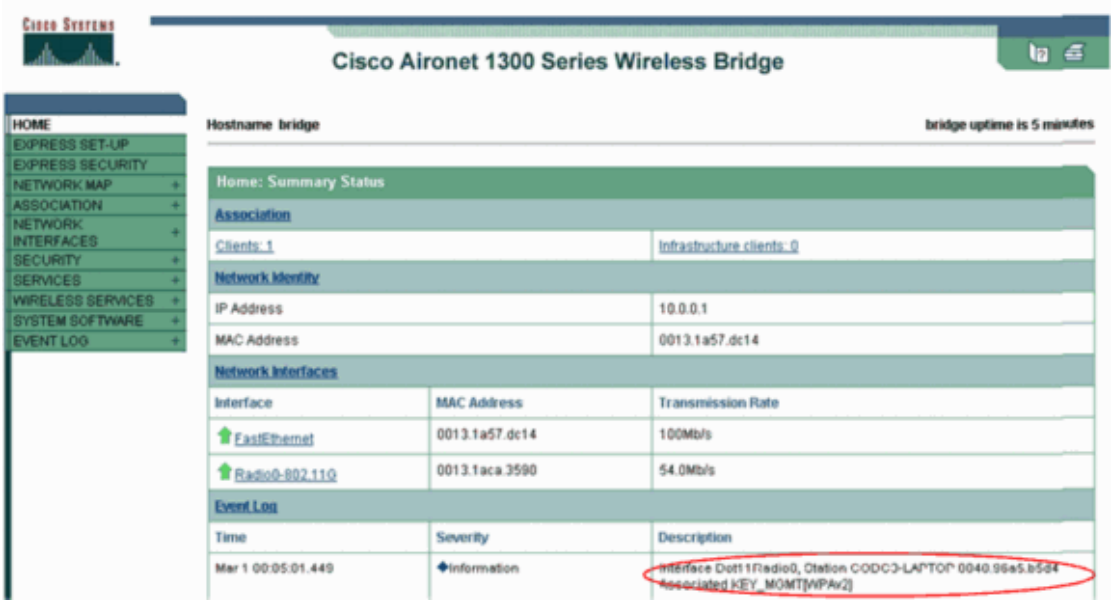
2. 选择状态检测认证情况



3. 选择 ADU 的状态，检测 AES 加密以及 LEAP 的认证情况



4. 选择 AP 的配置见面，检查 log，检查相应客户的关联情况



排错

对于上述配置暂时无排错信息

个人模式配置

在个人模式时，使用 PSK 作认证，此方法要在 AP 和客户端手工配置 PSK 的认证密钥。PSK 的认证使用密码在客户端和 AP 之间作认证，不需要专门的认证服务器。当客户端密码与 AP 上的密码一致时才能访问网络。密码同时也用作通过 TKIP 或者 AES 对数据包进行加密的关键字，个人模式适合在 SOHO 等相对安全性不高的环境下使用，以下将介绍在个人模式下如何配置 WPA2。

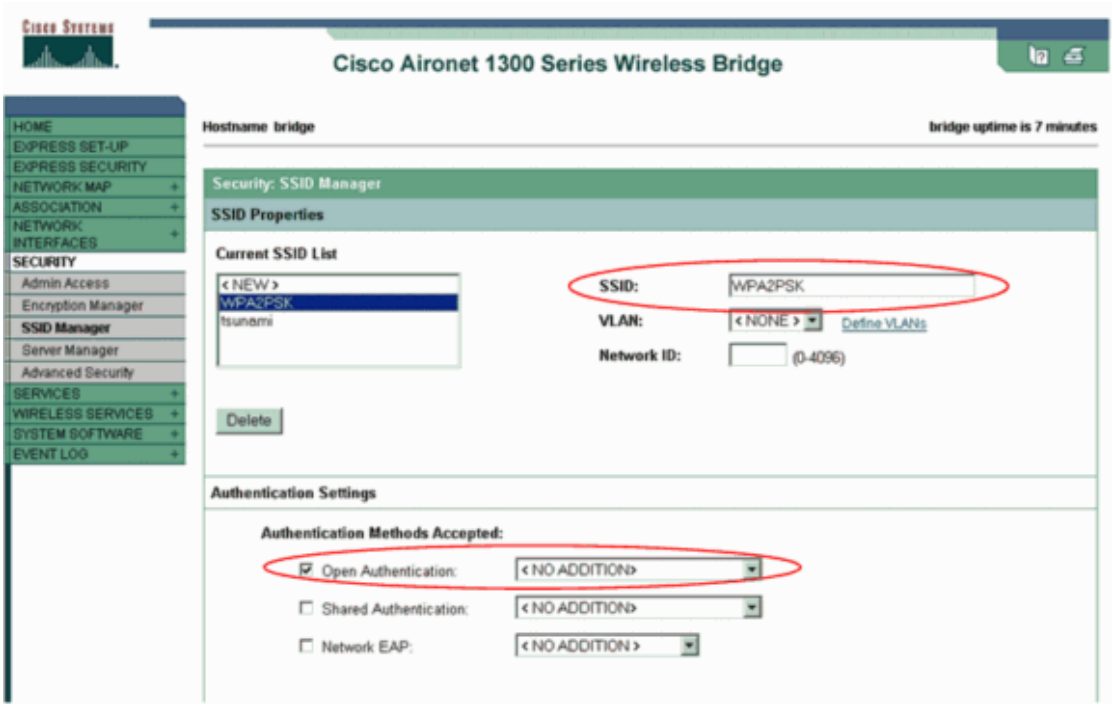
网络配置

在这个例子中,一个客户将会通过 WPA2 的客户端和 1310AP 认证,使用 WPA2 PSK 做认证,采用 AES-CCMP 的加密方法。

配置 AP

1. 选择 Security > Encryption Manager
   A. 选择 AES CCMP
   B. 点 Apply

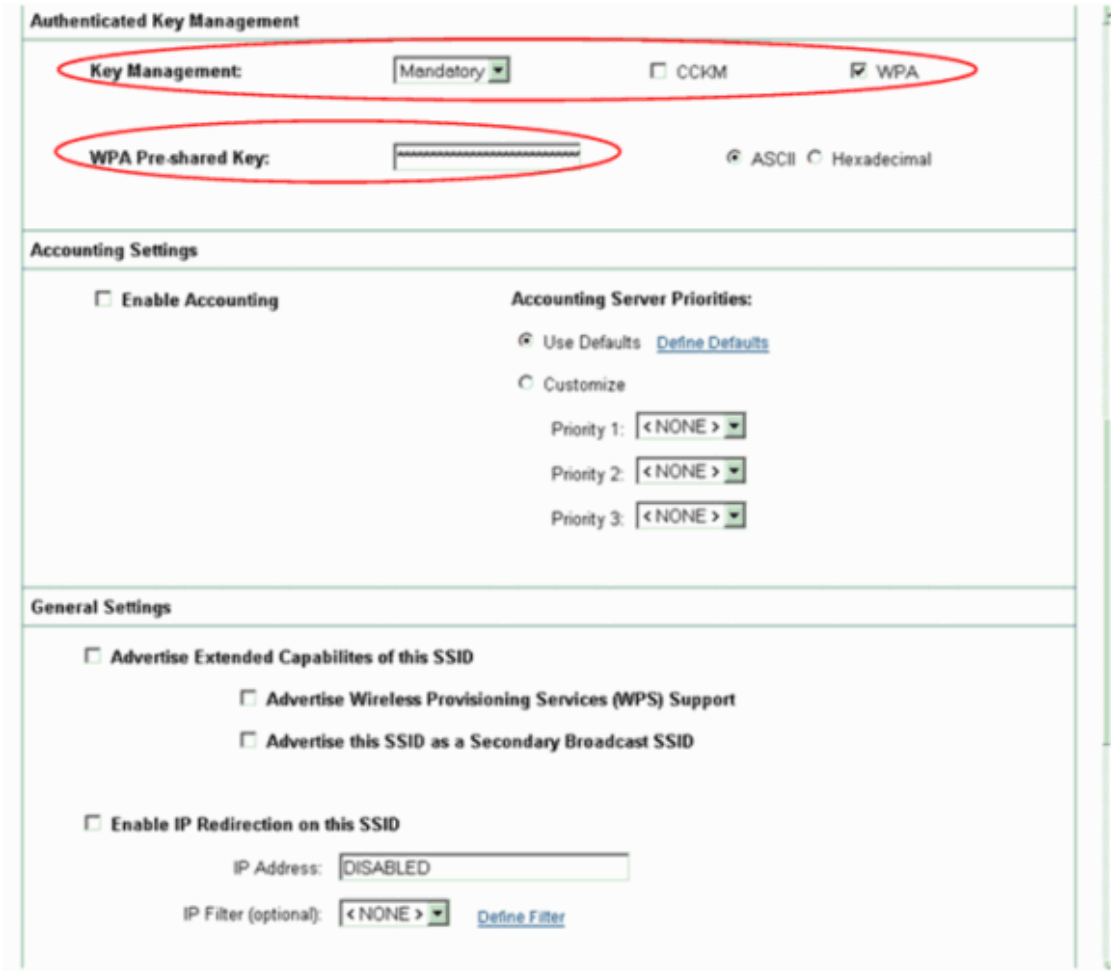
2. 选择 Security > SSID Manager 为 WPA2 应用创建一个新的 SSID
   A. 选择 Open Authentication



B. 下拉页面进入密码管理界面

A. 选择 Mandatory.

B. 选择 WPA

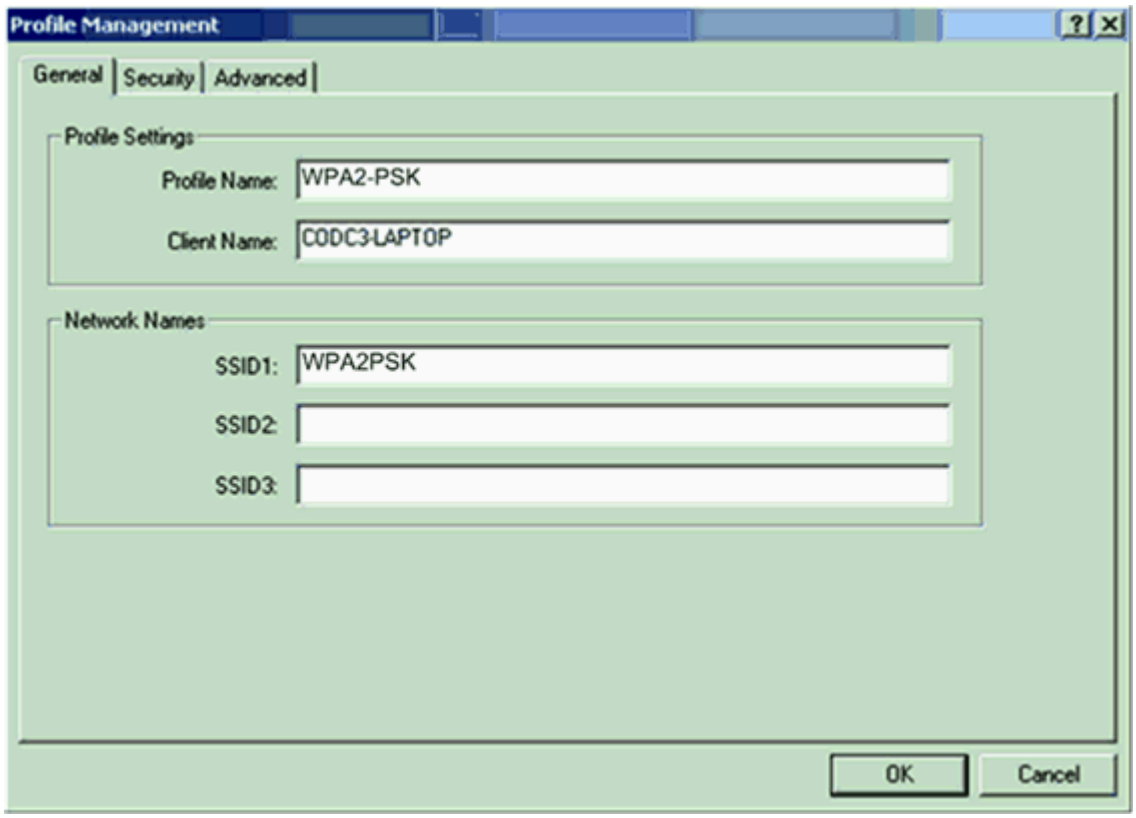


C. 输入 WPA PSK 密钥。这个密钥必需与配置在客户端上折 WPA PSK 密钥一致。

D. Apply

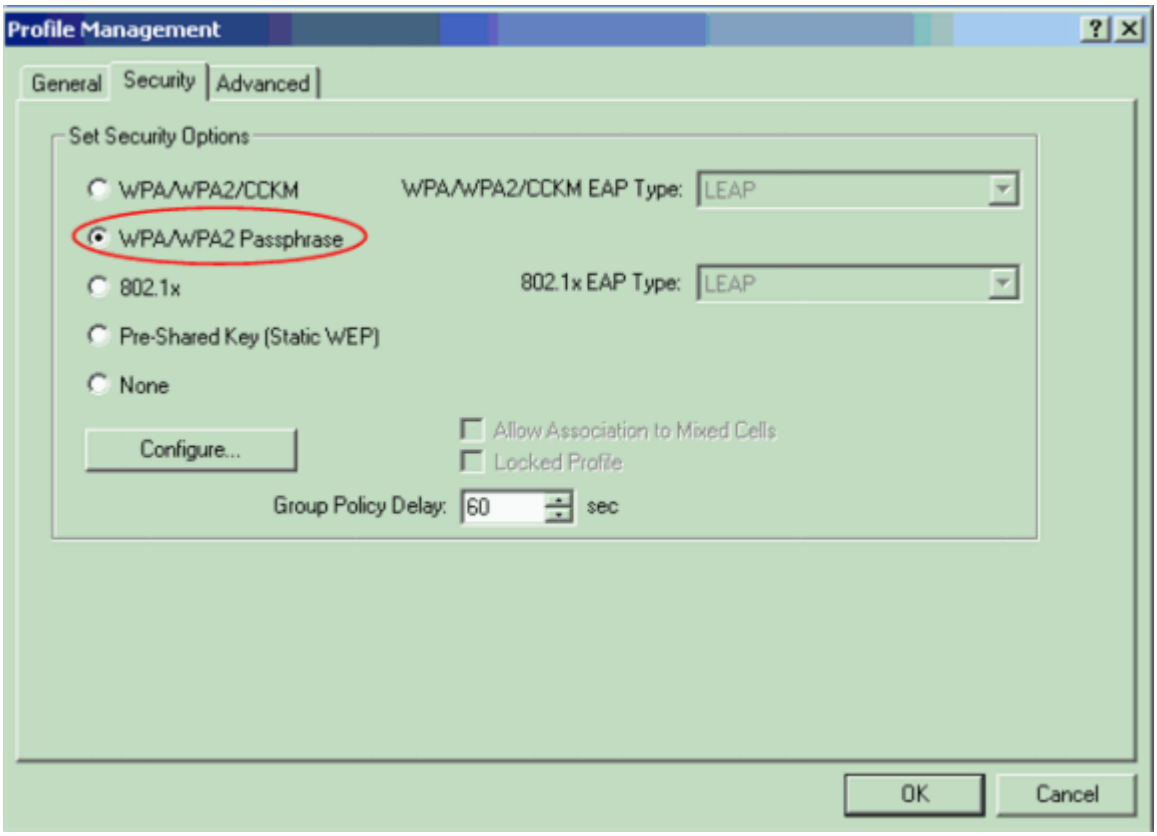
配置客户端

1. 在 ADU 客户端的帐户管理，选择 New



在这个例子中，Profile 名字和 SSID 均配置为 WPA2PSK.

2. 选择 Security，点击 WPA/WPA2 Passphrase.



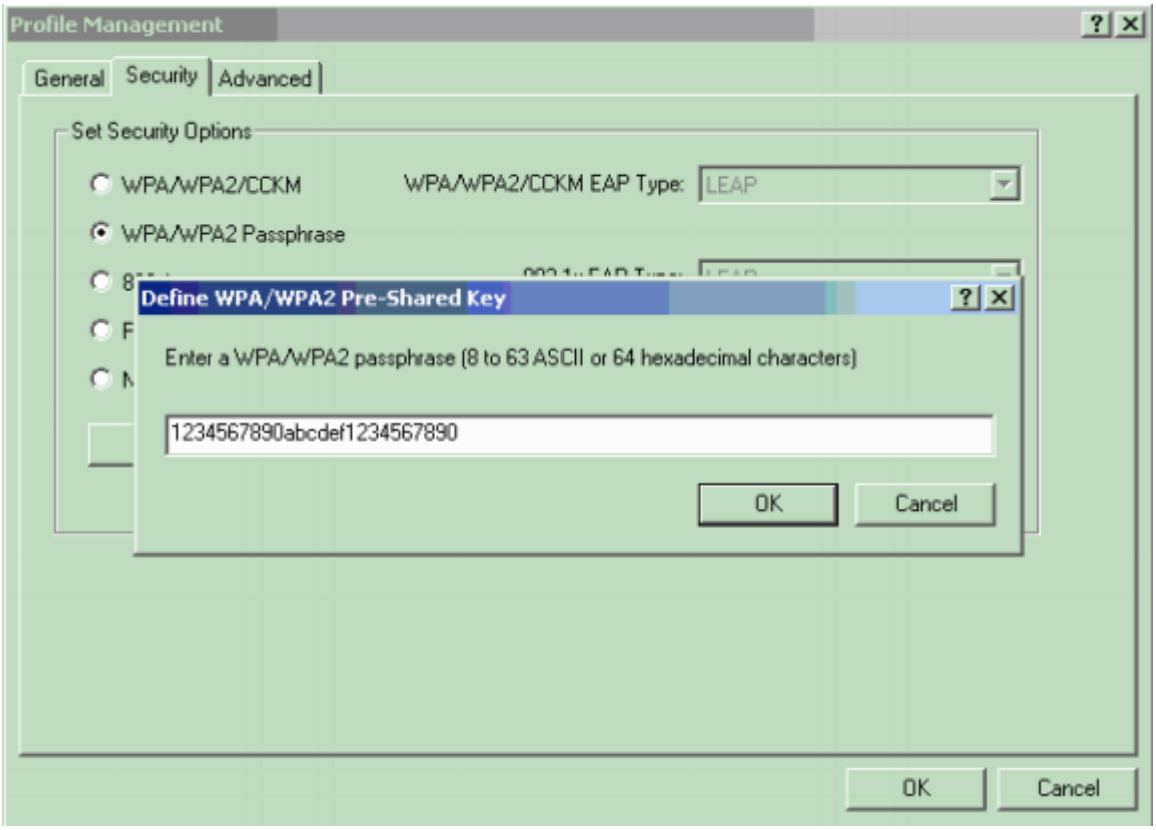
3. 点击 Configure.，配置 PSK 的密码

4. 获得系统管理员的权限，进入 WPA/WPA2 passphrase 里添加,PSK 的代码。

使用下面的规则输入通行代码

WPA/WPA2 passphrase 必须是在 8 到 63 的 ASCII 码，或是 64 位的 16 进制数。

客户端的配置必须要与 AP 上的代码相同

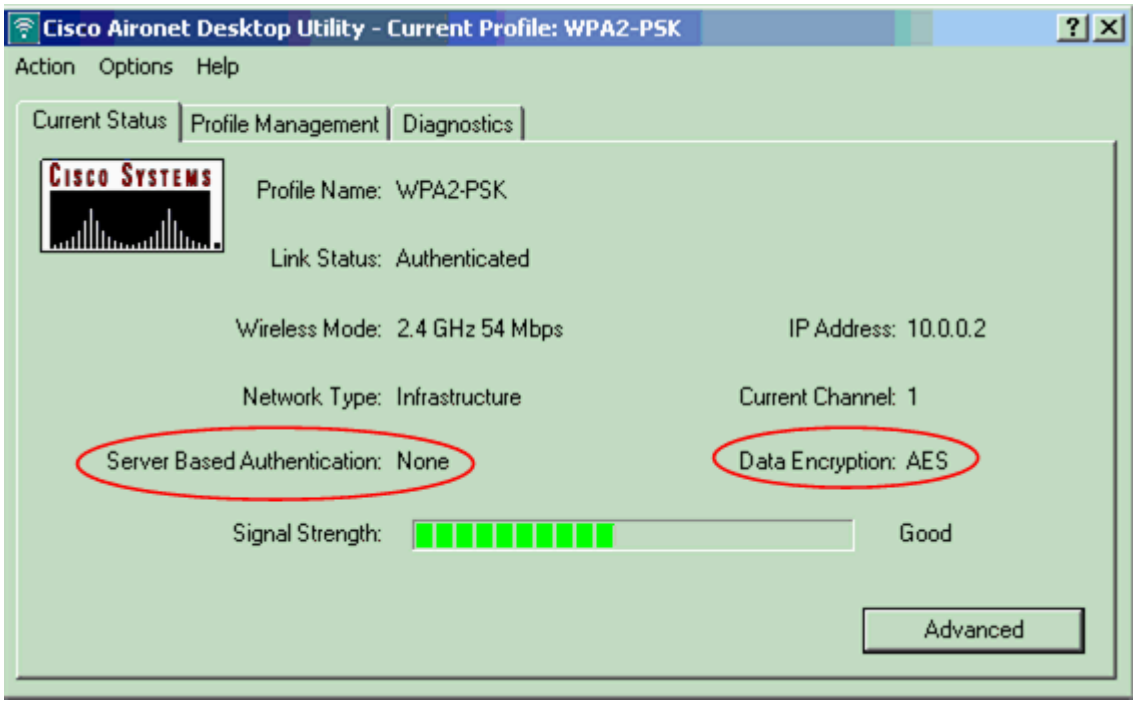


5. 点击 OK

检测

使用以下方法检测配置情况

1. 点击 ADU 的状态



2. 点击 AP 的配置界面，查看 Log 信息，检查客户端是否通过 WPA2 PSK 模式认证成功。

排错

对于上述配置暂时无排错信息