在无线局域网控制器配置示例的认证

Contents

Introduction

本文档提供了配置示例，说明如何在无线 LAN 控制器 (WLC) 中配置不同类型的第 1 层、第 2 层和第 3 层身份验证方法。

Prerequisites

Requirements

尝试进行此配置之前，请确保满足以下要求：

- 了解轻量接入点 (LAP) 和 Cisco WLC 的配置
- 了解 802.11i 安全标准

Components Used

本文档中的信息基于以下软件和硬件版本：

- 运行固件版本6.0.182.0的Cisco 4400 WLC
- Cisco 1000 系列 LAP
- 运行固件版本 2.6 的 Cisco 802.11a/b/g 无线客户端适配器

- Cisco Secure ACS 服务器版本 3.2

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.

WLC 中的身份验证

Cisco 统一无线网络 (UWN) 安全解决方案将可能较复杂的第 1 层、第 2 层和第 3 层 802.11 接入点 (AP) 安全组件捆绑到一个简单的策略管理器，该管理器基于每个无线 LAN (WLAN) 自定义系统范围的安全策略。Cisco UWN 安全解决方案提供了简单、统一和系统化的安全管理工具。

可在 WLC 中实施这些安全机制。

第 1 层解决方案

根据连续失败尝试次数限制客户端访问。

第 2 层解决方案

无认证—当此选项从第2层安全下拉列表时被挑选，第2层认证在WLAN没有进行。这与 802.11 标准的开放式身份验证相同。

Static WEP — 在使用静态有线等效保密 (WEP) 的情况下，特定 WLAN 中的所有 AP 和客户端无线电 NIC 必须使用相同的加密密钥。传输前每个发送站使用 WEP 密钥加密每个帧的正文，接收站在收到帧时使用相同的密钥对其进行解密。

802.1x — 配置 WLAN 以使用基于 802.1x 的身份验证。使用 IEEE 802.1X 提供了一个有效框架，以便验证和控制要发送至受保护网络的用户流量，以及动态更改加密密钥。802.1X 将称为可扩展身份验证协议 (EAP) 的协议绑定到有线和 WLAN 媒体，并支持多种身份验证方法。

Static WEP + 802.1x — 此第 2 层安全设置启用 802.1x 和静态 WEP。客户端可使用静态 WEP 或 802.1x 身份验证来连接到网络。

Wi-Fi 保护访问 (WPA) — WPA 或 WPA1 及 WPA2 是来自 Wi-Fi 联盟的基于标准的解决方案，该解决方案为 WLAN 系统提供数据保护和访问控制。WPA1 与 IEEE 802.11i 标准兼容，但是它在该标准得到承认之前已实施。WPA2 是 Wi-Fi 联盟对承认的 IEEE 802.11i 标准的实施。

默认情况下，WPA1 使用临时密钥完整性协议 (TKIP) 和消息完整性检查 (MIC) 进行数据保护。WPA2 使用更强大的高级加密标准加密算法，该算法将计数器模式和密码块链消息身份验证码协议 (AES-CCMP) 结合使用。默认情况下，WPA1 和 WPA2 都使用 802.1X 进行身份验证密钥管理。但是，以下这些选项也是可用的：PSK、CCKM 和 CCKM+802.1x。如果选择 CCKM，则 Cisco 仅允许使用支持 CCKM 的客户端。如果选择 CCKM+802.1x，则 Cisco 还允许使用非 CCKM 客户端。

CKIP —Cisco锁上完整性协议(CKIP)是加密的802.11媒体的一个Cisco专利的安全协议。CKIP 使用密钥置换、MIC 和消息序列号提高了 802.11 在基础架构模式中的安全性。软件版本 4.0 支持使用静态密钥的 CKIP。要使此功能正确运行，必须为 WLAN 启用 Aironet 信息元素 (IE)。WLAN 中指

定的 CKIP 设置对于尝试关联的所有客户端都是必需的。如果 WLAN 配置为使用 CKIP 密钥置换和 MMH MIC，则客户端必须支持这二者。如果 WLAN 配置为仅使用其中一项功能，则客户端必须仅支持该 CKIP 功能。WLC 仅支持静态 CKIP（与静态 WEP 一样）。WLC 不支持使用 802.1x 的 CKIP（动态 CKIP）。

第 3 层解决方案

什么都—当此选项从第3层安全下拉列表时被挑选，第3层认证在WLAN没有进行。

Note: 无身份验证部分中介绍了无第 3 层身份验证和无第 2 层身份验证的配置示例。

Web 策略（Web 身份验证和 Web 传递） — Web 身份验证通常供要部署来宾访问网络的客户使用。在来宾访问网络中，存在初始用户名和口令身份验证，但后续流量无安全要求。典型部署可以包括“热点”位置，如 T-Mobile 或 Starbuck。

对 Cisco WLC 的 Web 身份验证在本地进行。创建一个接口，然后将 WLAN/服务集标识符 (SSID) 与该接口相关联。

Web 身份验证提供简单的身份验证，无需请求方或客户端。请记住，Web 身份验证不提供数据加密。Web 身份验证通常用作仅关注连接性的“热点”或校园环境的简单访客接入。

Web 传递是一项解决方案，无线用户通过该解决方案重定向到可接受的使用策略页，当他们连接到 Internet 时无需进行身份验证。该重定向由 WLC 自行处理。唯一的要求是为 Web 传递配置 WLC，Web 传递基本上是无需输入任何凭据的 Web 身份验证。

VPN 传递 — VPN 传递是一项功能，它允许客户端仅与特定的 VPN 服务器建立隧道。因此，如果您需要安全地访问已配置的 VPN 服务器以及另一台 VPN 服务器或 Internet，则通过在控制器中启用 VPN 传递无法实现该目的。

在以下各部分中，为每种身份验证机制提供了配置示例。

配置示例

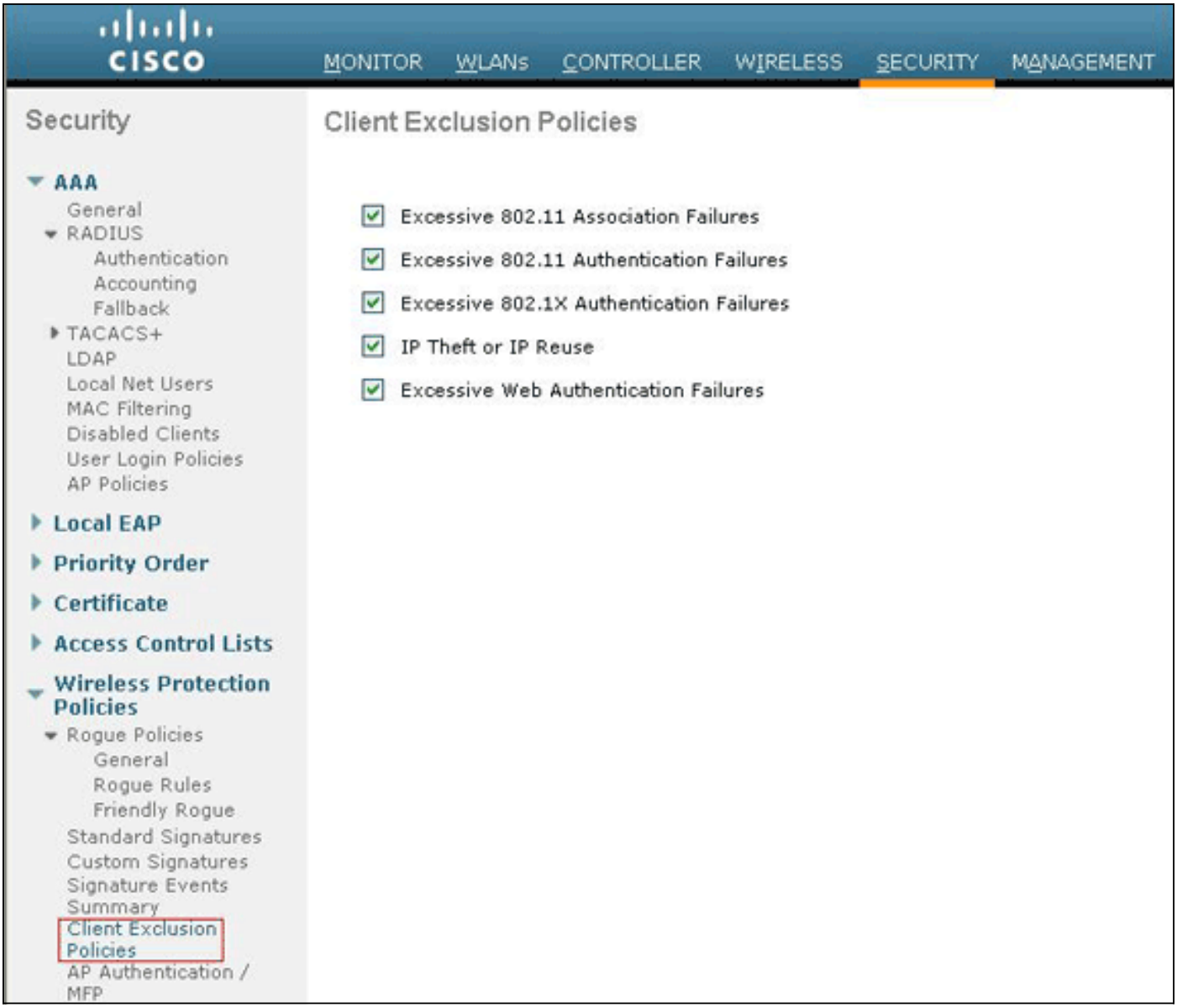
在配置 WLAN 和身份验证类型之前，必须配置 WLC 进行基本操作并在 WLC 中注册 LAP。本文档假设已配置 WLC 进行基本操作，并且已在 WLC 中注册 LAP。如果您是尝试设置 WLC 以对 LAP 执行基本操作的新用户，请参阅在无线 LAN 控制器 (WLC) 中注册轻量 AP (LAP)。

第 1 层安全解决方案

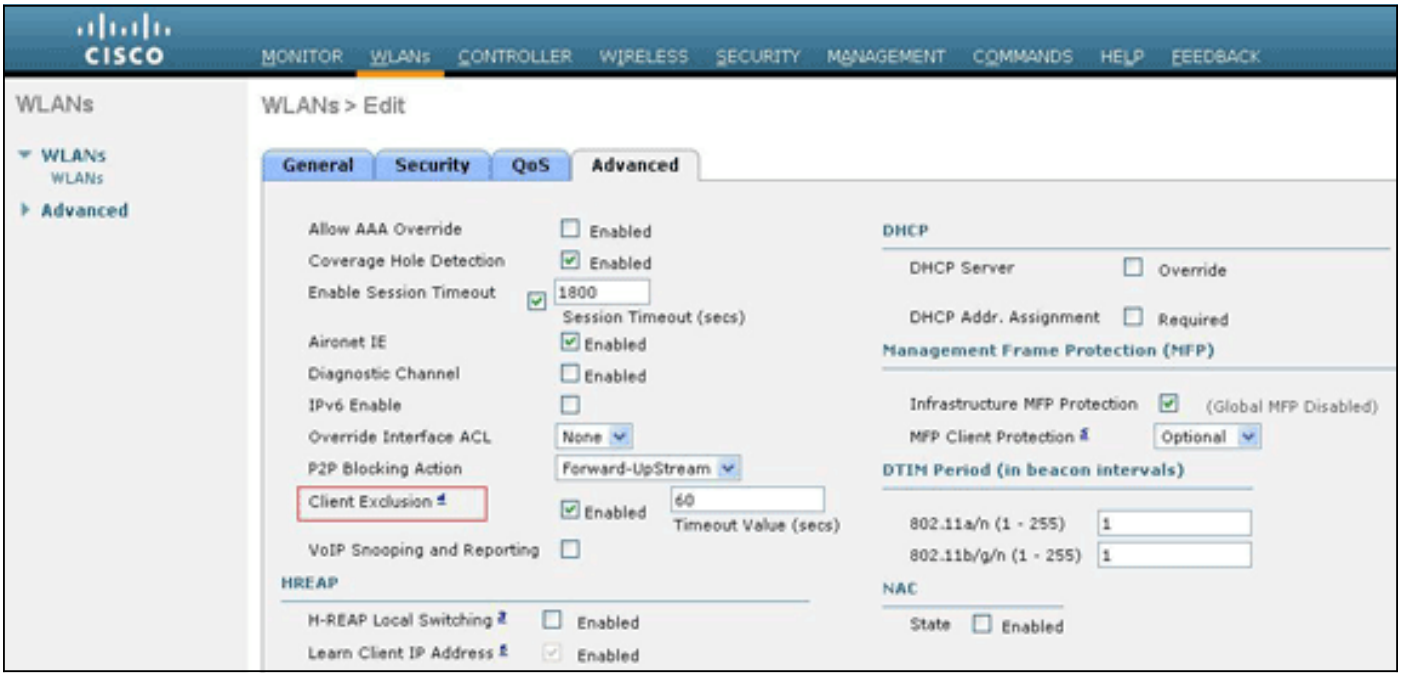
根据访问 WLAN 网络的连续失败尝试次数，可以限制无线客户端的访问。默认情况下，符合这些条件将发生客户端排除。无法更改这些值。

- 连续的 802.11 身份验证失败（连续 5 次，排除第 6 次尝试）
- 连续的 802.11 关联失败（连续 5 次，排除第 6 次尝试）
- 连续的 802.1x 身份验证失败（连续 3 次，排除第 4 次尝试）
- 外部策略服务器故障
- 尝试使用已分配给其他设备的 IP 地址（IP 盗用或 IP 重用）
- 连续的 Web 身份验证（连续 3 次，排除第 4 次尝试）

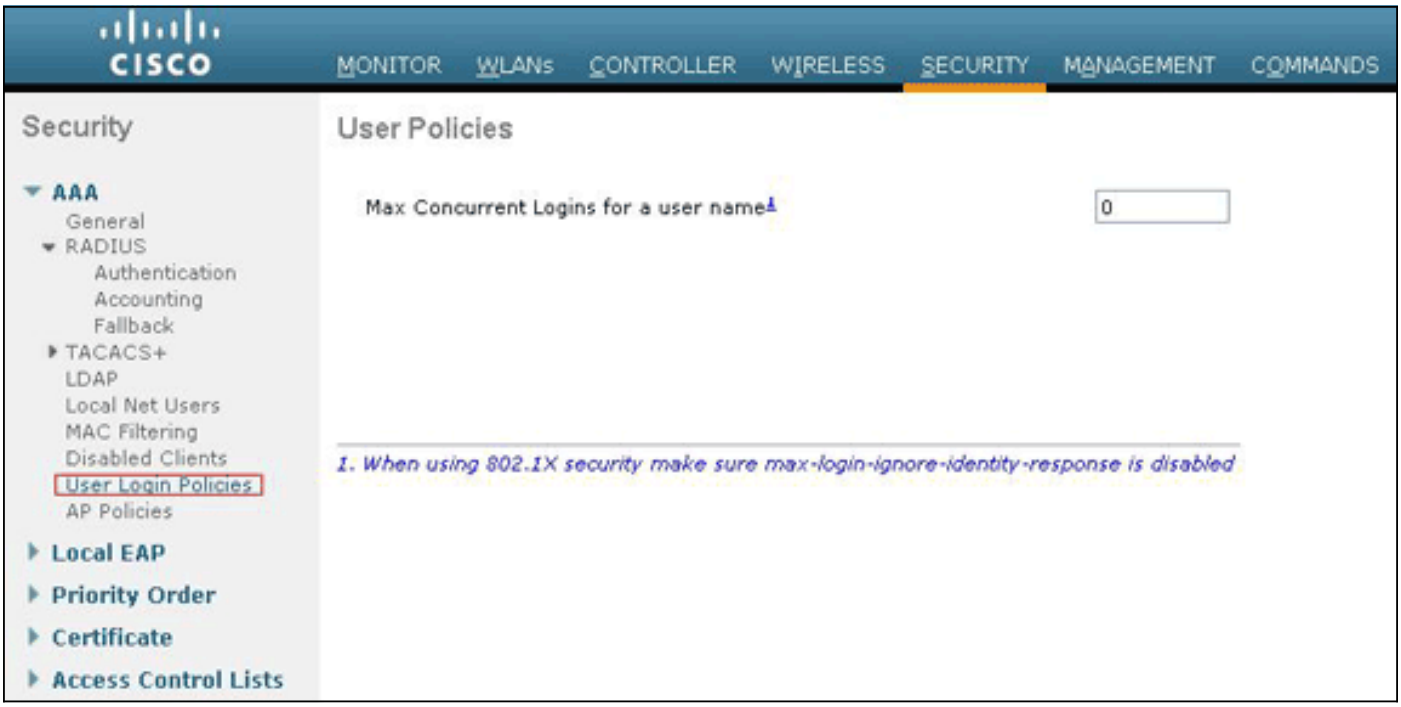
为了找出客户端排除策略，请点击在顶部菜单的**安全**，在页的左边然后选择**无线保护策略>客户端排除策略**定位。



可以配置排除计时器。可针对每个控制器启用或禁用排除选项。可针对每个 WLAN 启用或禁用排除计时器。



默认情况下，单个用户名的最大并发登录数为 0。您可以输入 0 和 8 之间的任何值。此参数可以在 **SECURITY > AAA > User Login Policies** 中进行设置，并且允许您为单个客户端名称指定最大并发登录数（在 1 和 8 之间或者 0 =无限制）。示例如下：

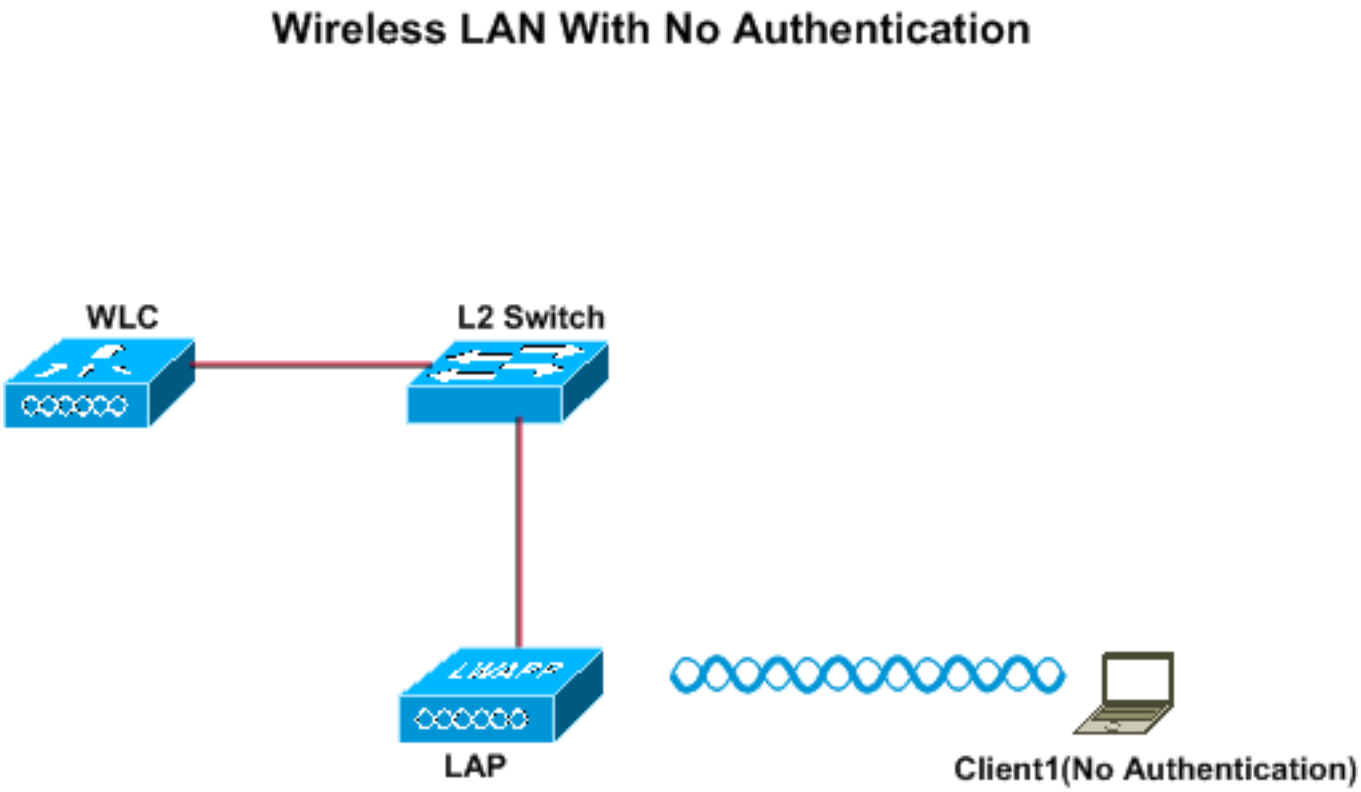


第 2 层安全解决方案

无身份验证

此示例显示一WLAN被配置，不用认证。

Note: 本示例也适用于“无第 3 层身份验证”。

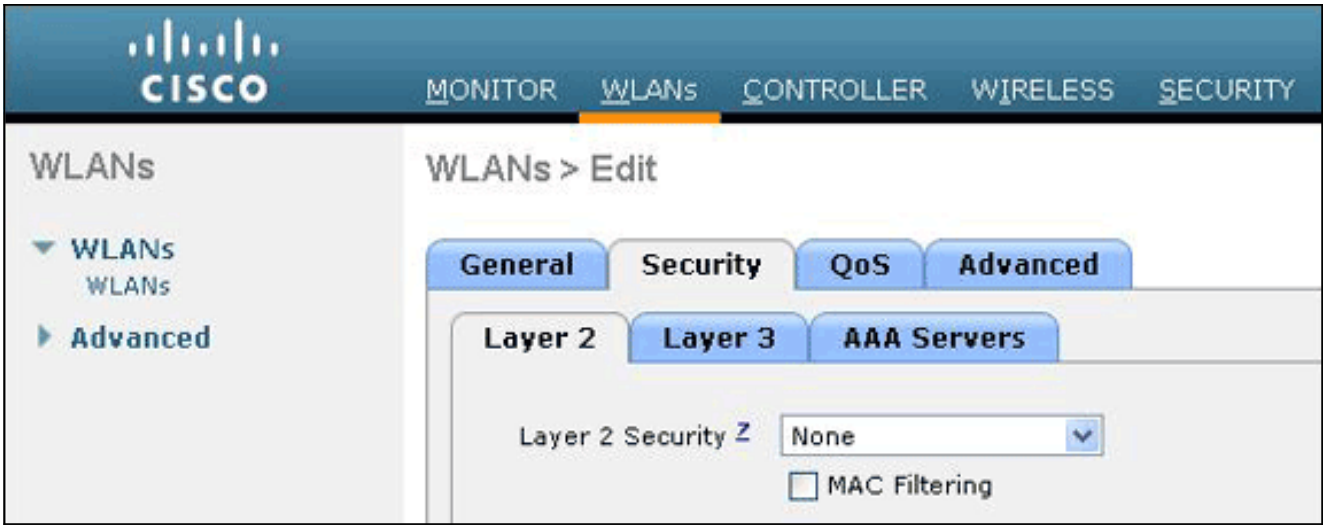


配置 WLC 使用无身份验证

要配置 WLC 使用该设置，请完成以下步骤：

1. 要创建 WLAN，请从控制器 GUI 中单击 **WLANs**。随即显示 WLAN 窗口。该窗口列出了控制器中配置的 WLAN。
2. 点击**去**为了配置一新的WLAN。
3. 输入WLAN的参数。此示例显示此WLAN的配置。

4. 单击 **Apply**。
5. 在“WLAN”>“Edit”窗口中，定义特定于该 WLAN 的参数。
6. 请勿点击**安全**选项，并且为第2层和第3层安全选择。



Note: 为了使变得激活的WLAN，状态应该是启用的。对enable (event)它，检查**Status复选框**在一般选项下。这将为该 WLAN 启用无身份验证。

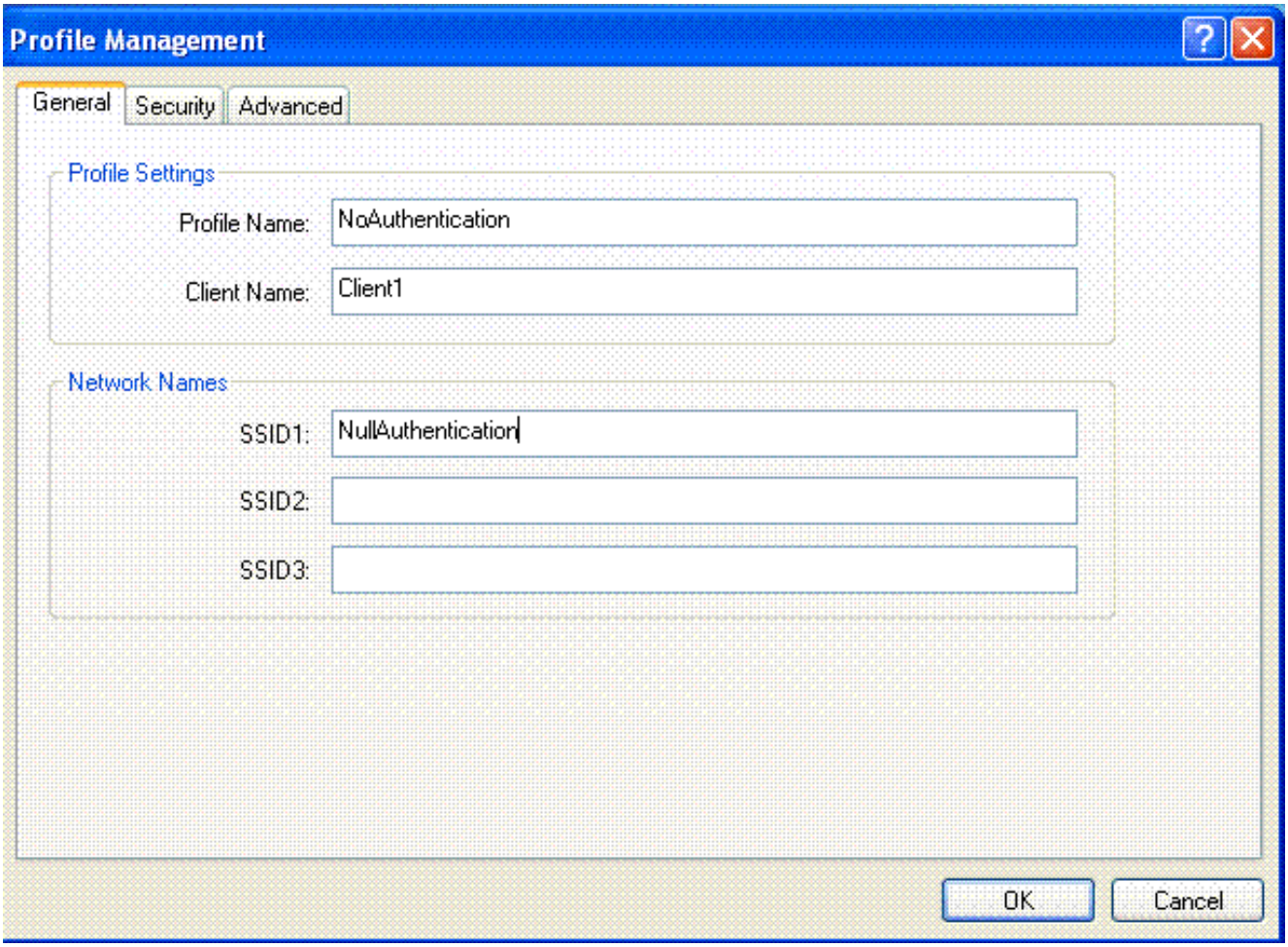
7. 选择根据您的设计需求的其他参数。此示例使用默认值。
8. 单击 **Apply**。

配置无线客户端使用无身份验证

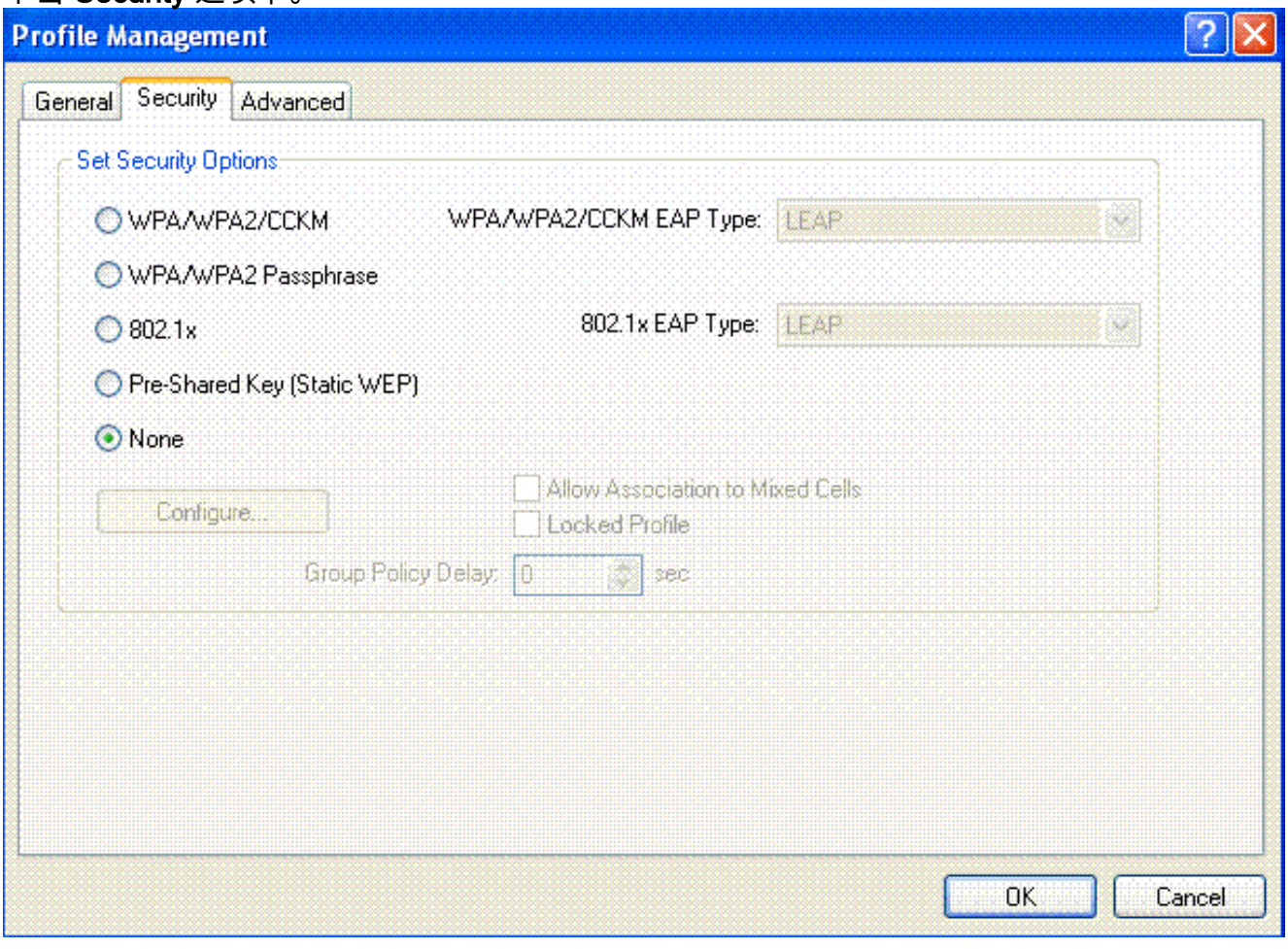
完成这些步骤为了配置此设置的无线局域网客户端：

Note: 本文使用运行固件3.5并且解释客户端适配器配置有ADU版本3.5的Aironet 802.11a/b/g客户端适配器。

1. 要创建新配置文件，请单击 ADU 上的 **Profile Management** 选项卡。
2. 点击 **New（新建）**。
3. 当配置文件管理(一般)时窗口显示，请完成这些步骤为了设置配置文件名字、客户端名和SSID：在“Profile Name”字段中输入配置文件的名称。此示例使用*NoAuthentication*作为配置文件名字。在“Client Name”字段中输入客户端的名称。客户端名称用于标识 WLAN 网络中的无线客户端。此配置使用*Client1*客户端名。以网络名，请输入是使用此配置文件的SSID。该 SSID 与您在 WLC 中配置的 SSID 相同。本示例中的 SSID 为 NullAuthentication。

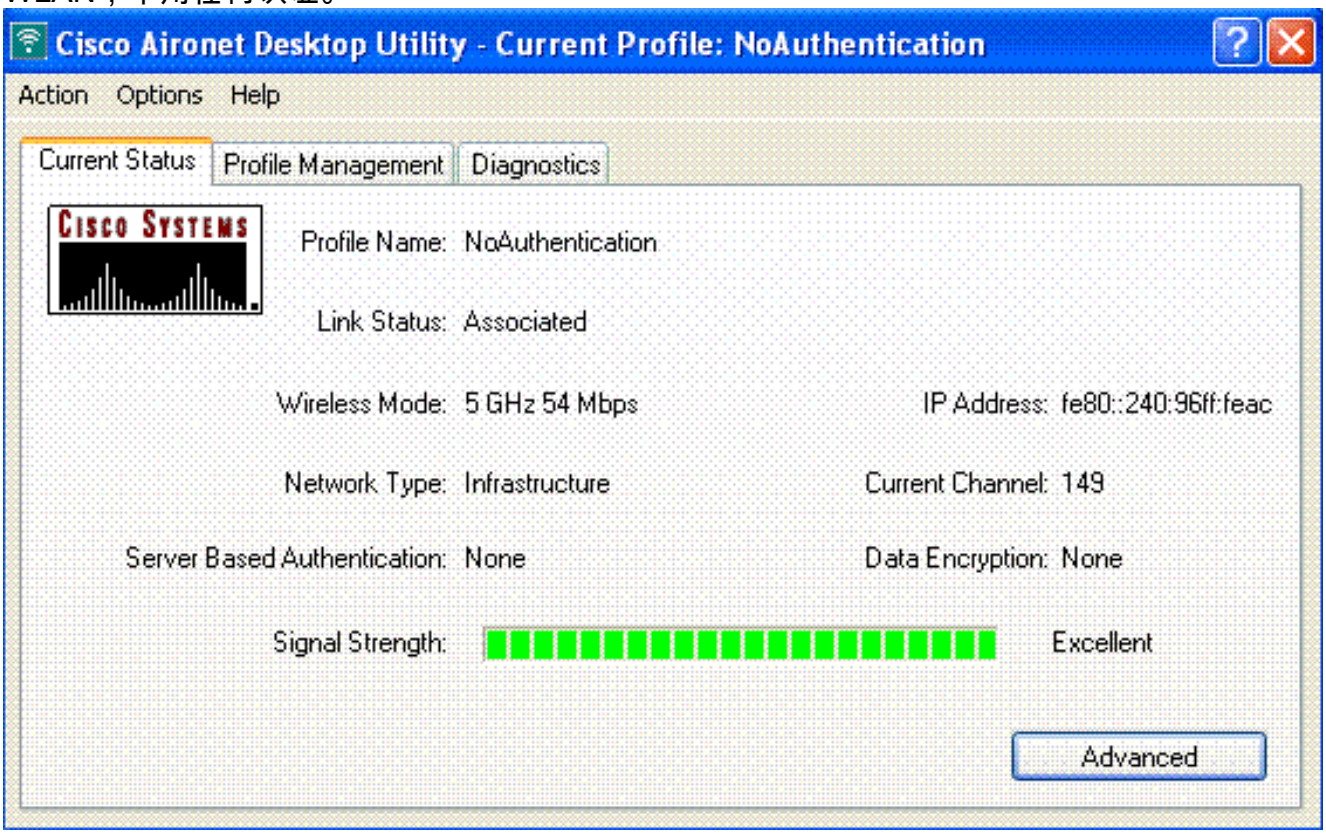


4. 单击 **Security** 选项卡。



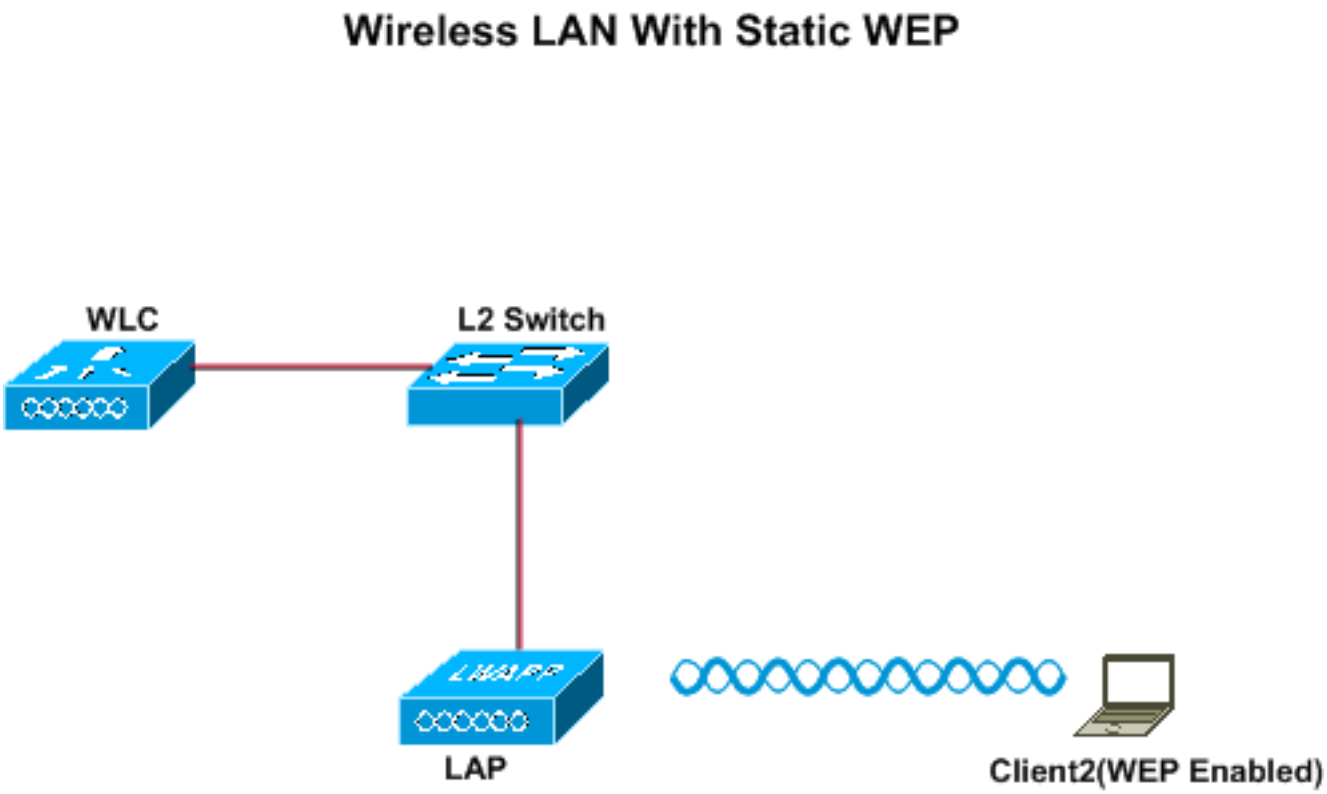
5. 请勿点击单选按钮在集安全选项下，然后点击OK键。当激活时SSID，无线客户端连接到

WLAN，不用任何认证。



静态 WEP

此示例显示一WLAN配置有静态WEP。



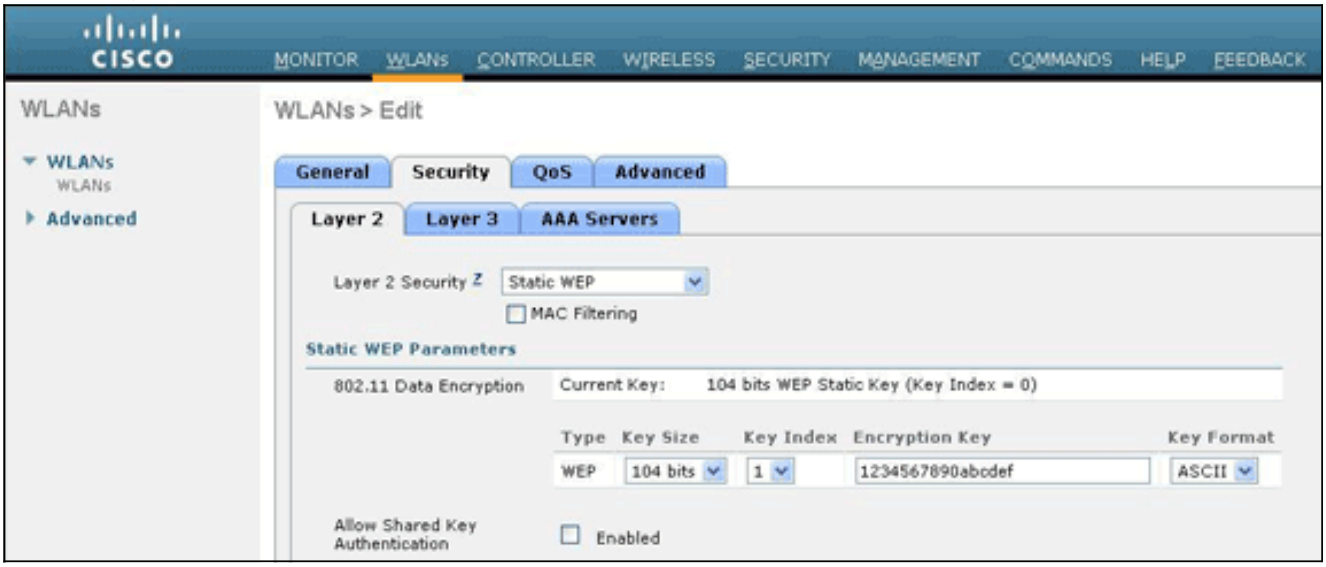
配置 WLC 使用静态 WEP

要配置 WLC 使用该设置，请完成以下步骤：

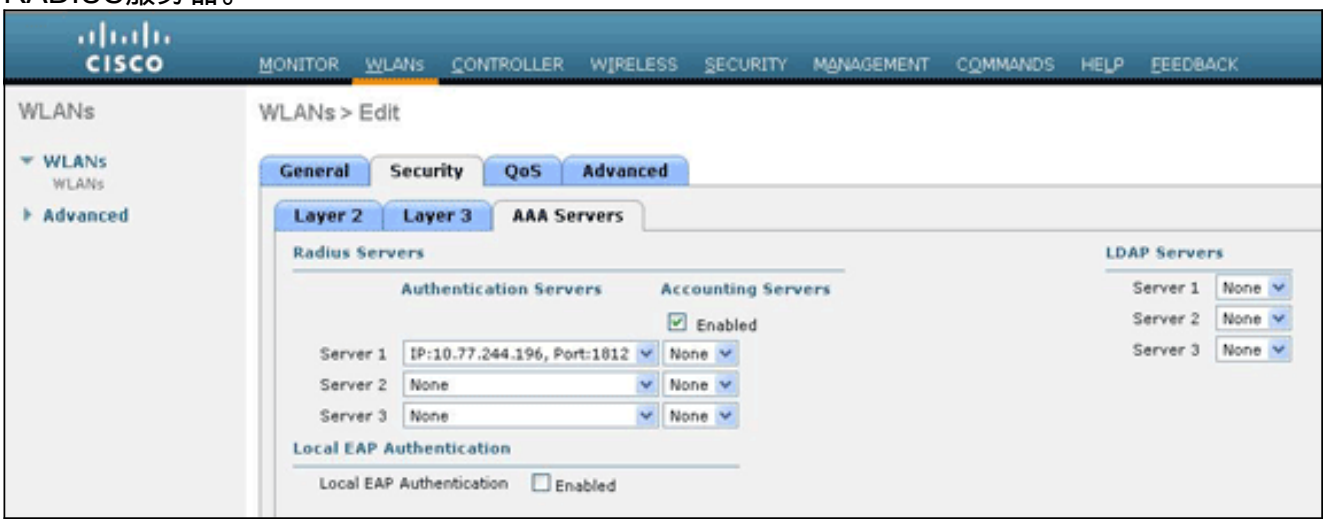
1. 要创建 WLAN，请从控制器 GUI 中单击 **WLANs**。随即显示 WLAN 窗口。该窗口列出了控制器中配置的 WLAN。
2. 要配置新的 WLAN，请单击 **New**。
3. 输入 WLAN ID 和 WLAN SSID。在本示例中，WLAN 的名称为 StaticWEP，WLAN ID 为 2。

4. 单击 **Apply**。
5. 在“WLAN”>“Edit”窗口中，定义特定于该 WLAN 的参数。从第2层下拉列表，请选择**静态 WEP**。这将为该 WLAN 启用静态 WEP。在静态WEP参数下，请选择WEP密钥大小和主索引

，并且输入静态WEP加密密钥。密钥大小可以是40位或104位。密钥索引可以介于 1 和 4 之间。可以对每个 WLAN 应用一个唯一的 WEP 密钥索引。由于只有四个 WEP 密钥索引，因此只有四个 WLAN 可以配置静态 WEP 第 2 层加密。在本示例中，使用 104 位的 WEP，所使用的 WEP 密钥为 1234567890abcdef。



检查RADIUS服务器是否为认证被配置。RADIUS服务器在**安全**选项可以被配置位于**AAA > Radius>认证**。一旦配置，应该分配RADIUS服务器到WLAN为认证。去**WLANs > Security >AAA服务器**为了分配RADIUS服务器到WLAN为认证。在本例中， 10.77.244.196是RADIUS服务器。



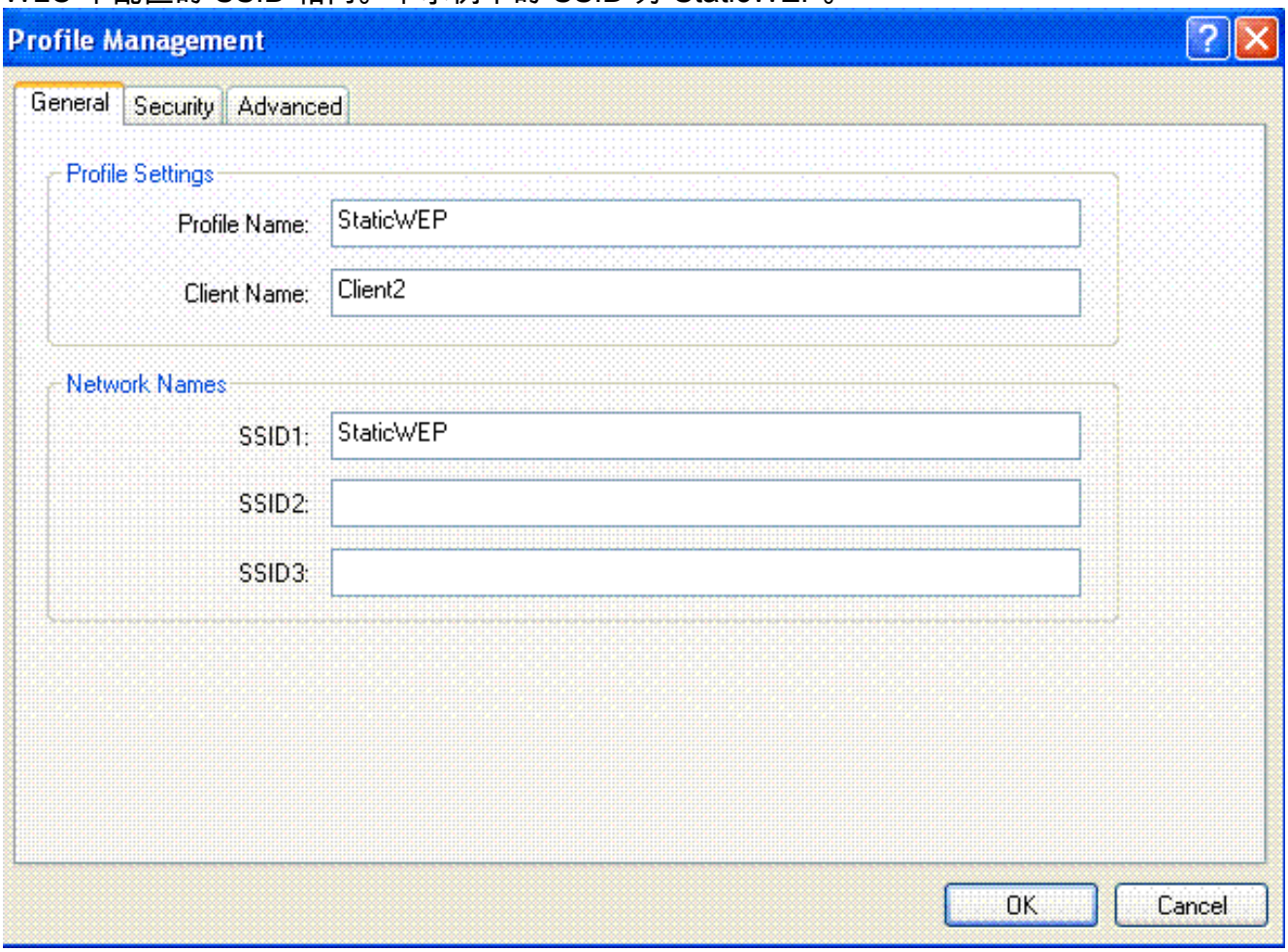
6. 选择根据您的设计需求的其他参数。此示例使用默认值。
7. 单击 **Apply**。**Note:** WEP在十六进制(十六进制)总是表示。当您在ASCII时输入WEP密钥，ASCII WEP字符串被转换成十六进制，用于加密信息包。没有供应商实行转换十六进制成ASCII的标准方法，因为一些将执行填充，而其他不。所以，最大供应商兼容性，您的WEP密钥的使用十六进制。**Note:** 如果要对 WLAN 启用共享密钥身份验证，请选中“Static WEP Parameters”下的 **Allow Shared-Key Authentication** 复选框。这样，如果将客户端也配置为使用共享密钥身份验证，在对数据包执行 WEP 加密之后，WLAN 中将对数据包进行共享密钥身份验证。

配置无线客户端使用静态 WEP

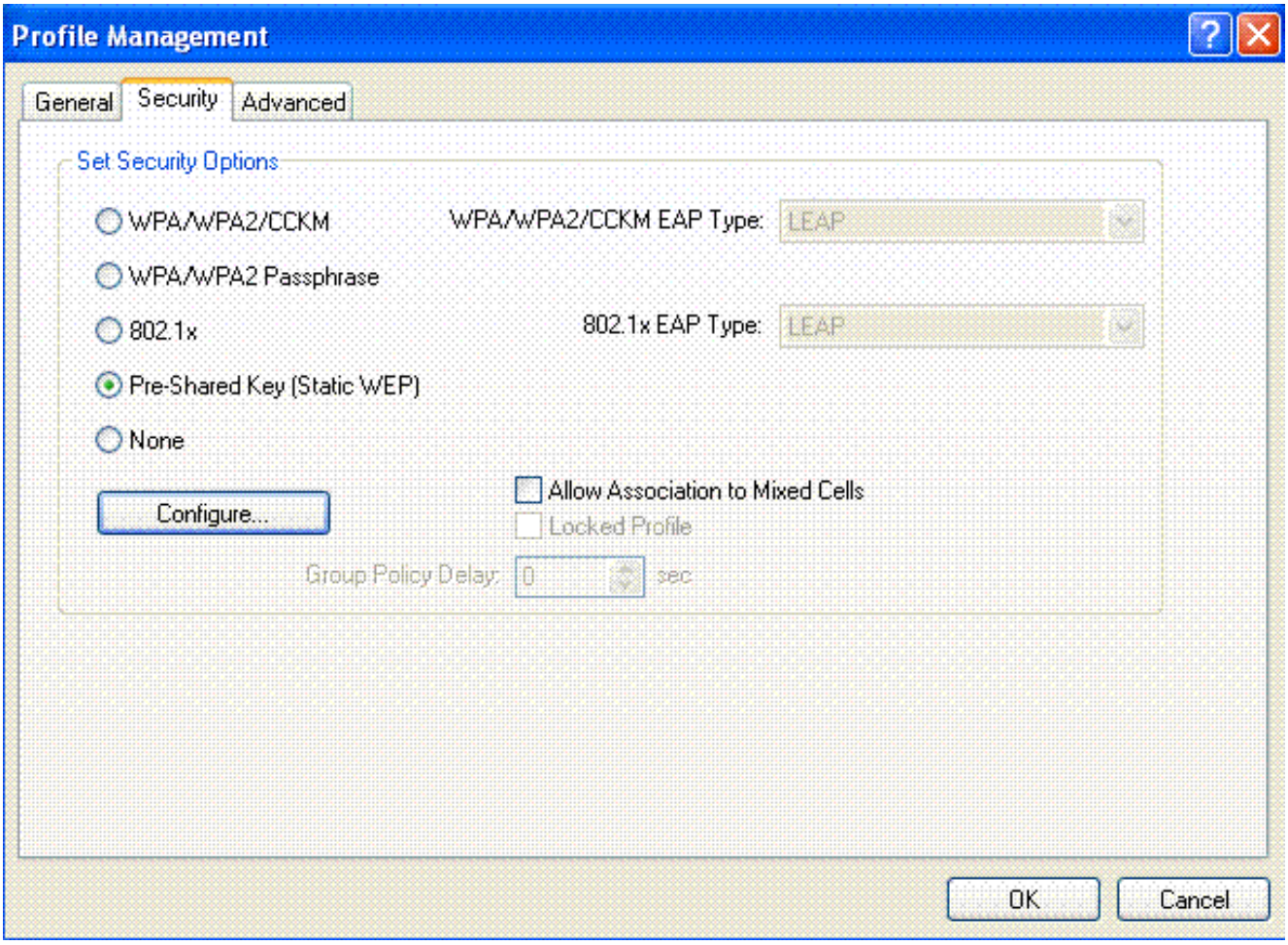
要配置无线 LAN 客户端使用该设置，请完成以下步骤：

1. 要创建新配置文件，请单击 ADU 上的 **Profile Management** 选项卡。

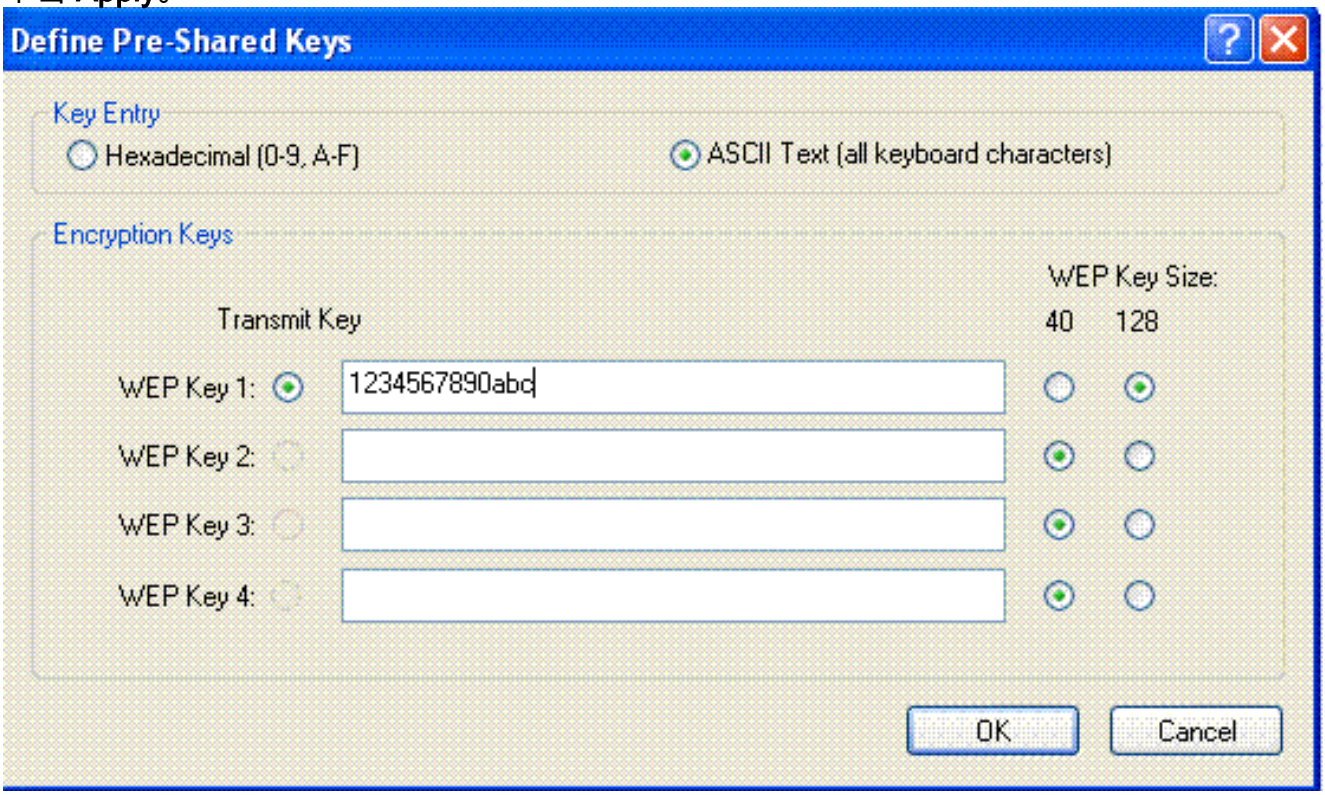
2. 点击 **New（新建）**。
3. 当配置文件管理(一般)时窗口显示，请完成这些步骤为了设置配置文件名字、客户端名和SSID：在“Profile Name”字段中输入配置文件的名称。此示例使用*StaticWEP*作为配置文件名字。在“Client Name”字段中输入客户端的名称。客户端名称用于标识 WLAN 网络中的无线客户端。此配置使用*Client2*客户端名。以网络名，请输入是使用此配置文件的SSID。该 SSID 与您在 WLC 中配置的 SSID 相同。本示例中的 SSID 为 StaticWEP。



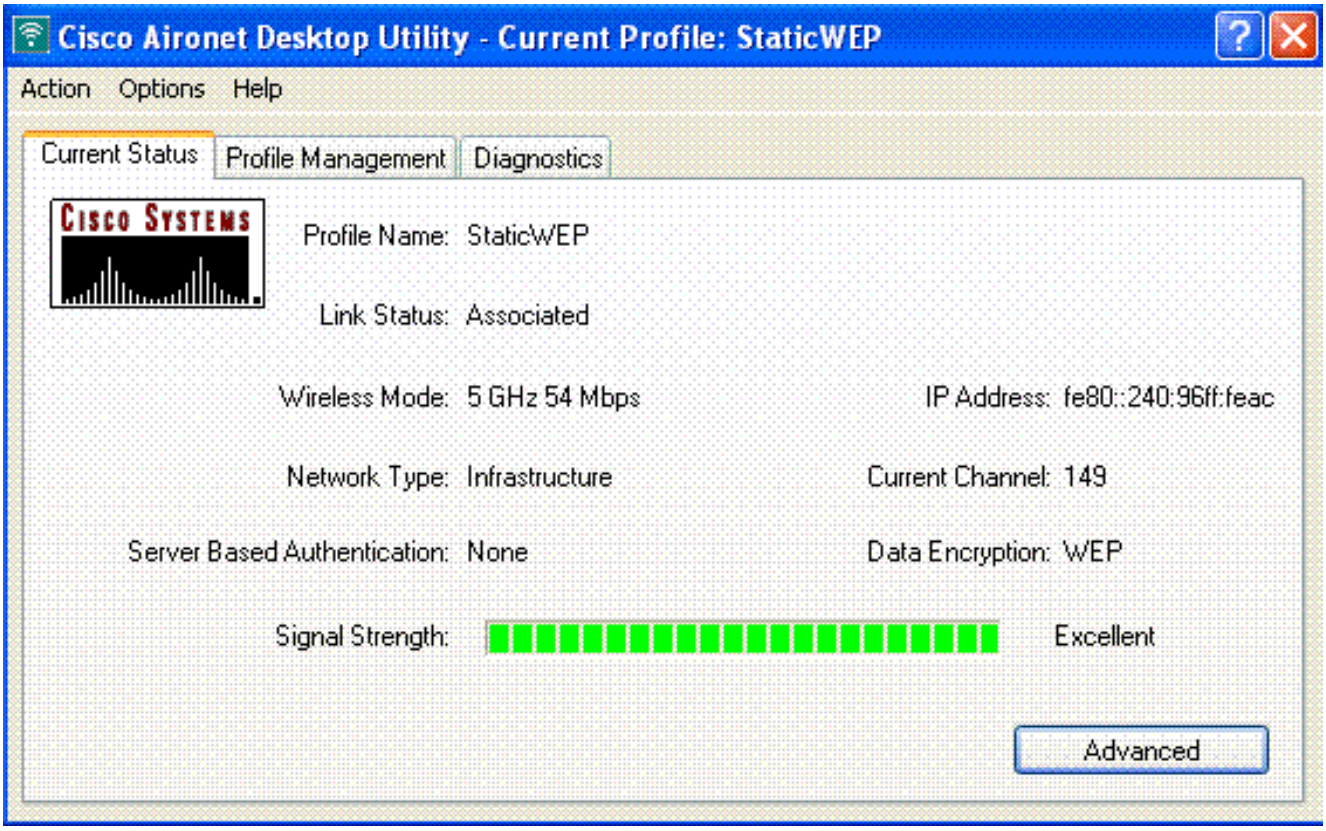
4. 单击 **Security** 选项卡。



5. 在“Set Security Options”下，选择 **Pre-Shared Key (Static WEP)**。
6. 点击**配置**，并且定义了WEP密钥大小和WEP密钥。这应该与在 WLC 中为该 WLAN 配置的 WEP 密钥相匹配。
7. 单击 **Apply**。

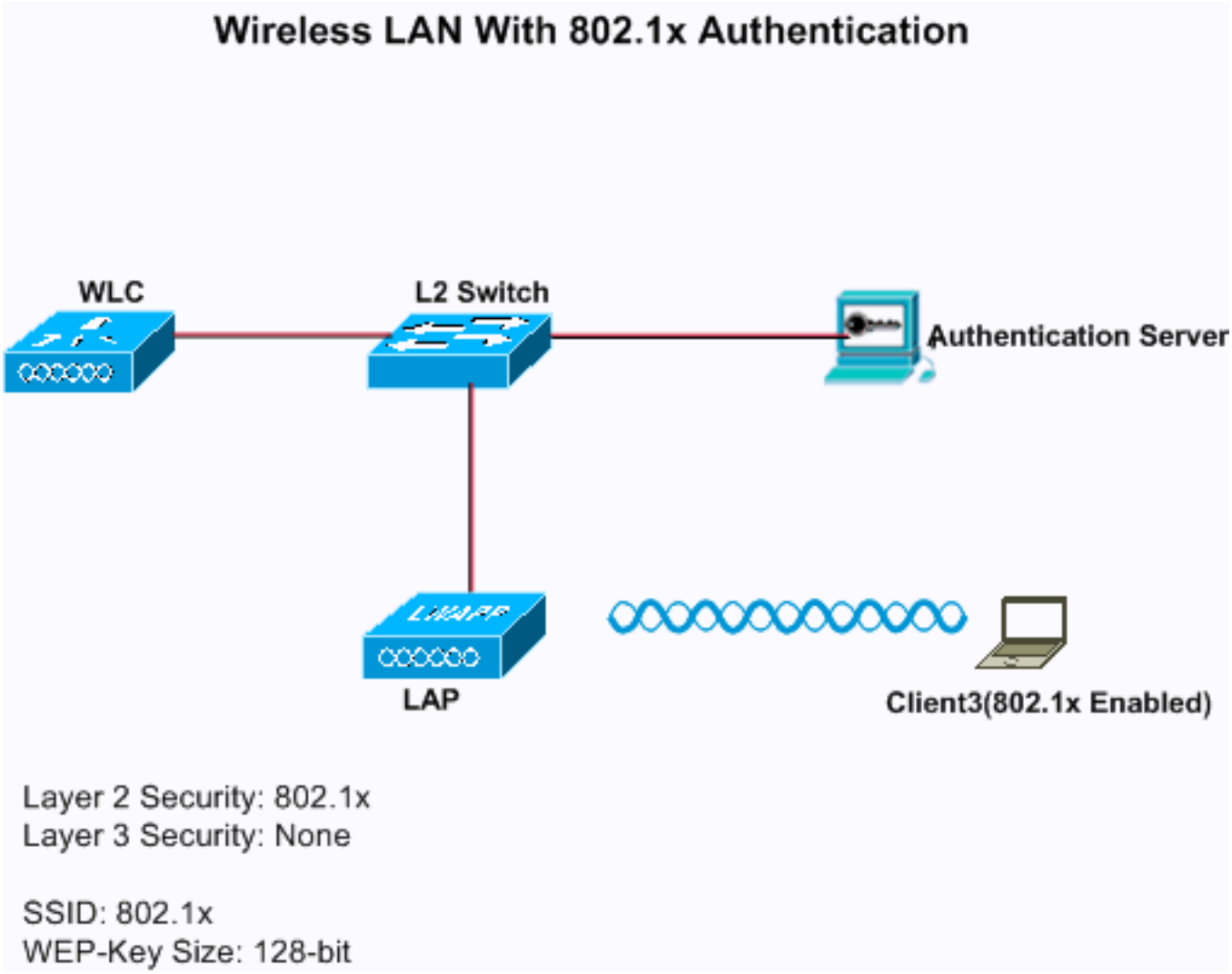


激活 SSID 后，无线客户端将连接到 WLAN 并且数据包将使用静态 WEP 密钥进行加密。



802.1x认证

此示例显示一WLAN配置有802.1x认证。



配置 WLC 使用 802.1x 身份验证

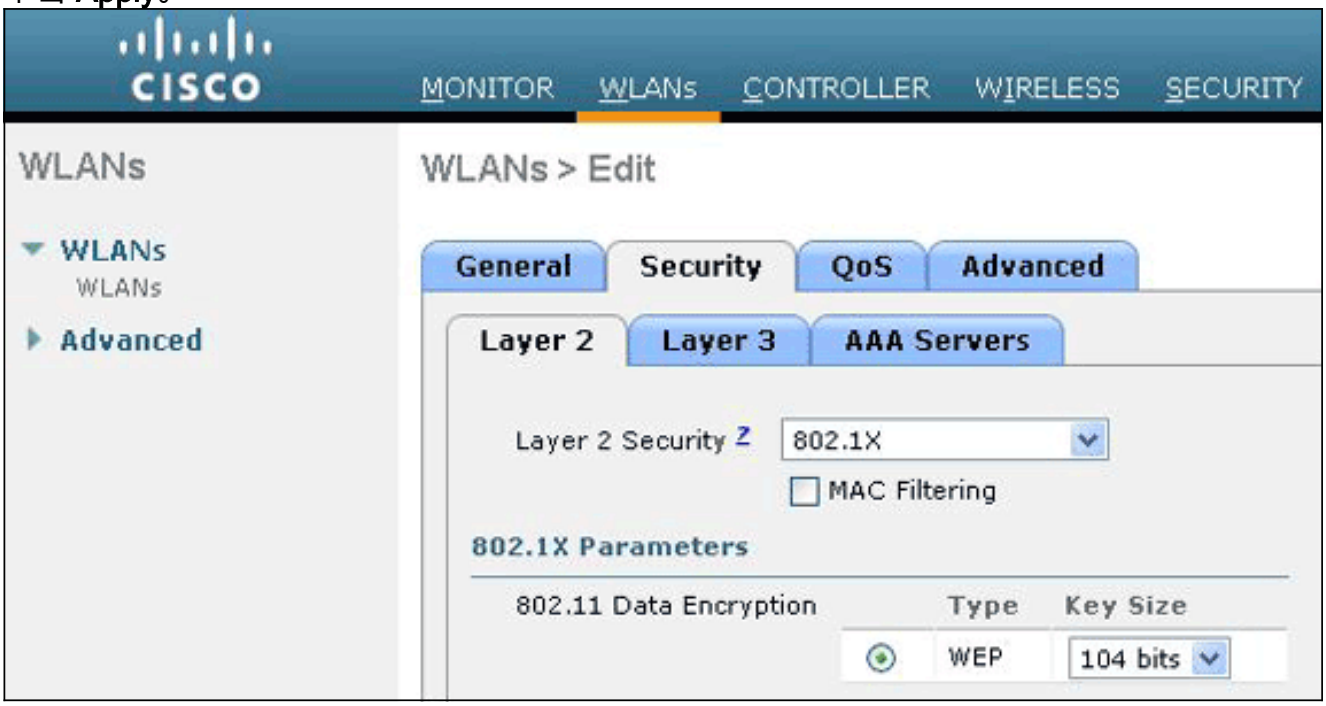
要配置 WLC 使用该设置，请完成以下步骤：

1. 要创建 WLAN，请从控制器 GUI 中单击 **WLANs**。随即显示 WLAN 窗口。该窗口列出了控制器中配置的 WLAN。
2. 要配置新的 WLAN，请单击 **New**。在本例中， WLAN被命名*802.1x*，并且WLAN ID是*3*。应该也添加配置文件名字。

3. 单击 **Apply**。
4. 在“WLAN”>“Edit”窗口中，定义特定于该 WLAN 的参数。从第2层下拉列表，请选择**802.1x**。**Note:** 仅WEP加密是可用的与802.1x。选择40位或104位加密的，并且确定第3层安全设置对无。这将为该 WLAN 启用 802.1x 身份验证。在RADIUS服务器参数下，请选择将使用验证客

户机证书的RADIUS服务器。选择根据您的设计需求的其他参数。此示例使用默认值。

5. 单击 **Apply**。

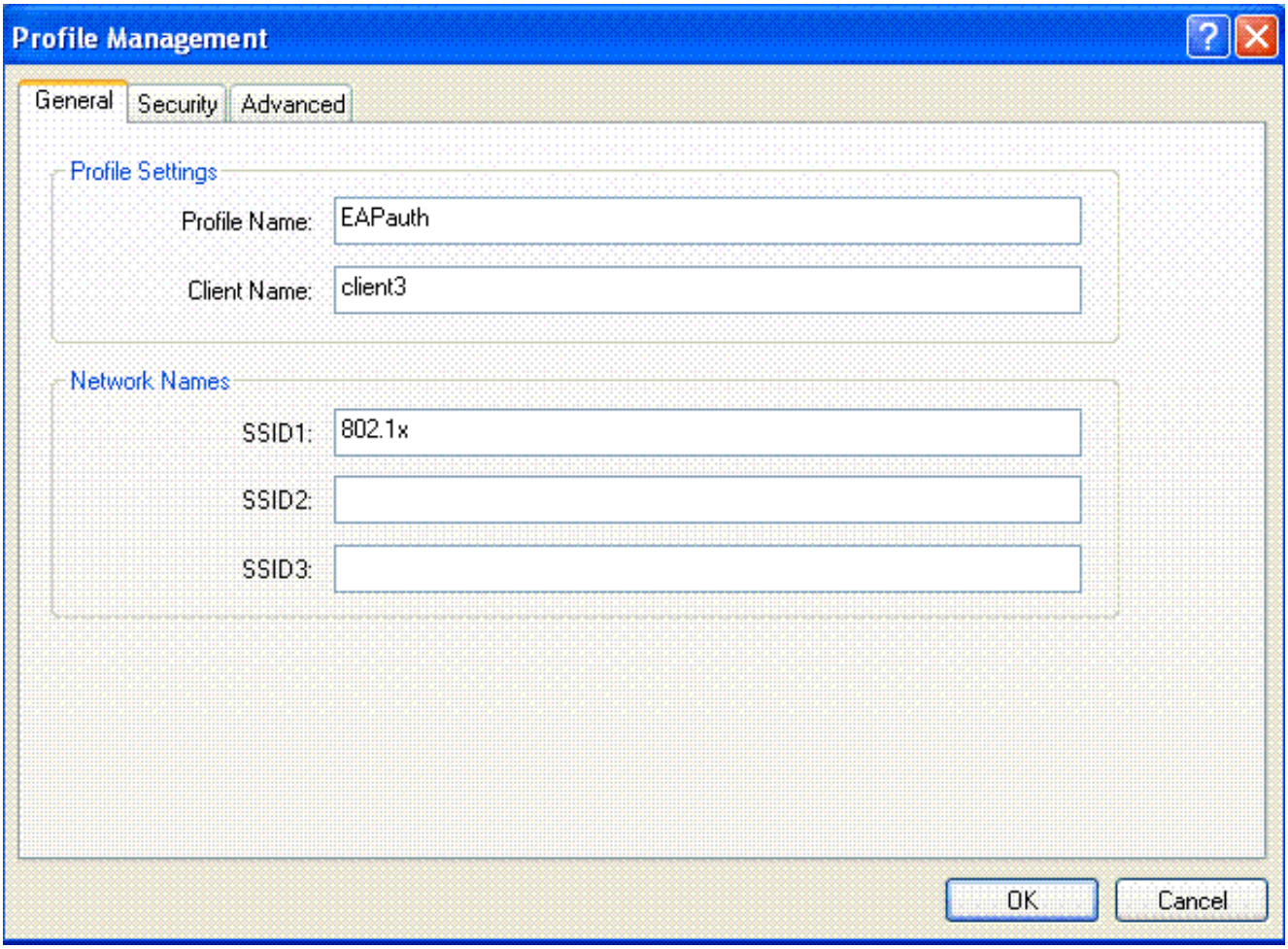


注意：如果选择第2层安全的*802.1x*，不可能使用CCKM。如果选择第2层安全的*WPA 1*或*WPA 2*，这些选项出现在Auth密钥管理下：*802.1x+CCKM* —如果选择此选项，支持CCKM或非CCKM客户端(可选的CCKM)。*802.1x* —如果选择此选项，只有支持802.1x客户端。*CCKM* —如果选择此选项，只有支持CCKM客户端，其中客户端处理到认证的一个外部服务器。*PSK* —如果选择此选项，预共享密钥使用WLC和客户端。并且，规定所有标准用于在预标准前;例如， WPA/WPA2采取在CCKM的先例，当同时使用。用于验证客户端的 EAP 身份验证类型取决于 RADIUS 服务器和无线客户端中配置的 EAP 类型。在 WLC 中启用 802.1x 后，WLC 允许所有类型的 EAP 数据包在 LAP、无线客户端和 RADIUS 服务器之间流动。以下文档提供了有关一些 EAP 身份验证类型的配置示例：[ACS 4.0 和 Windows 2003 中统一无线网络下的 PEAPACS 4.0 和 Windows 2003 中统一无线网络下的 EAP-TLS与WLAN控制器(WLC)配置示例的EAP验证]

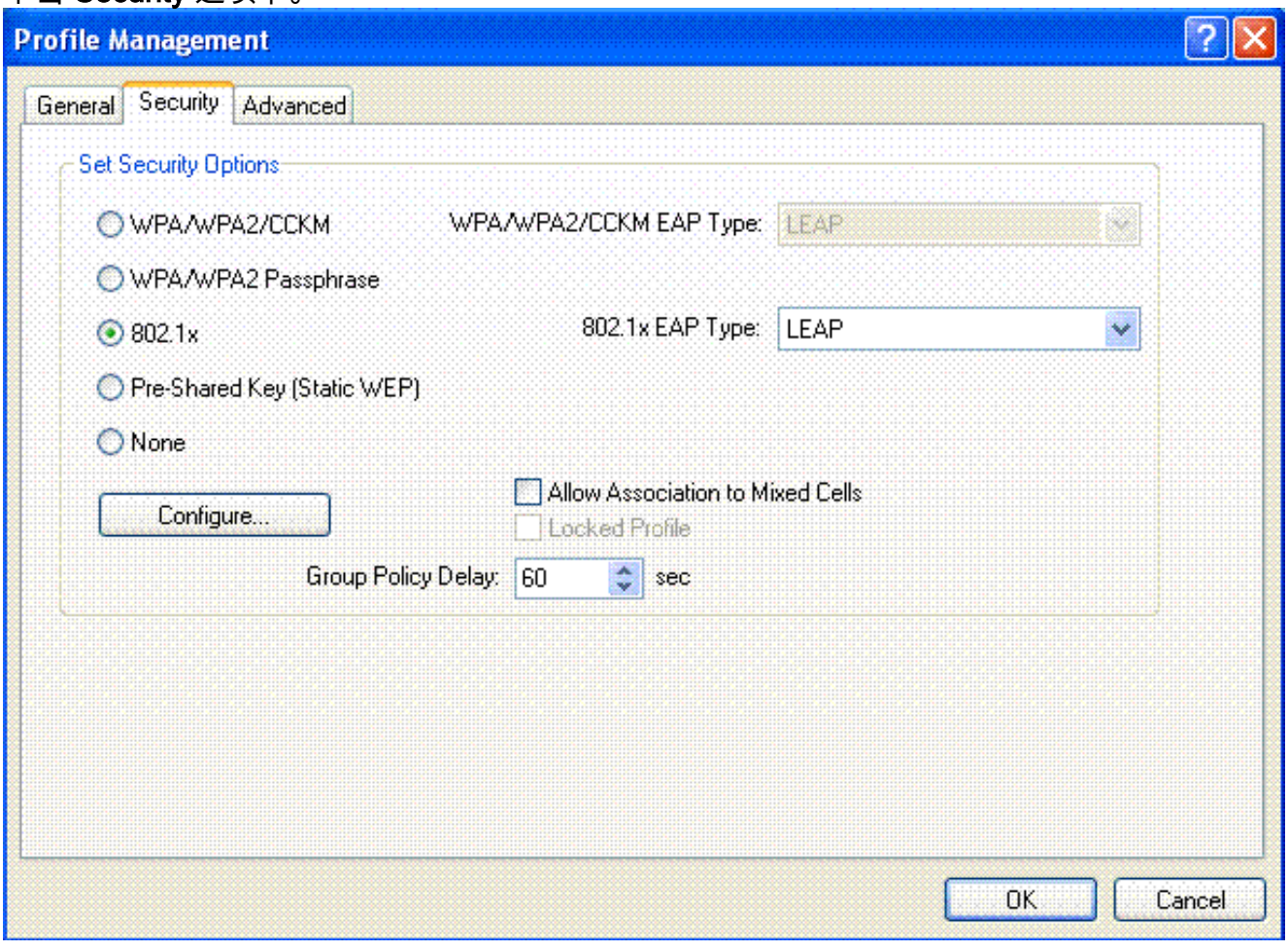
配置无线客户端使用 802.1x 身份验证

要配置无线 LAN 客户端使用该设置，请完成以下步骤：

1. 要创建新配置文件，请单击 ADU 上的 **Profile Management** 选项卡。
2. 点击 **New（新建）**。
3. 当配置文件管理(一般)时窗口显示，请完成这些步骤为了设置配置文件名字、客户端名和SSID：在“Profile Name”字段中输入配置文件的名称。此示例使用*EAPAuth*作为配置文件名字。在“Client Name”字段中输入客户端的名称。客户端名称用于标识 WLAN 网络中的无线客户端。此配置使用*Client3*客户端名。以网络名，请输入是使用此配置文件的SSID。该 SSID 与您在 WLC 中配置的 SSID 相同。本示例中的 SSID 为 802.1x。

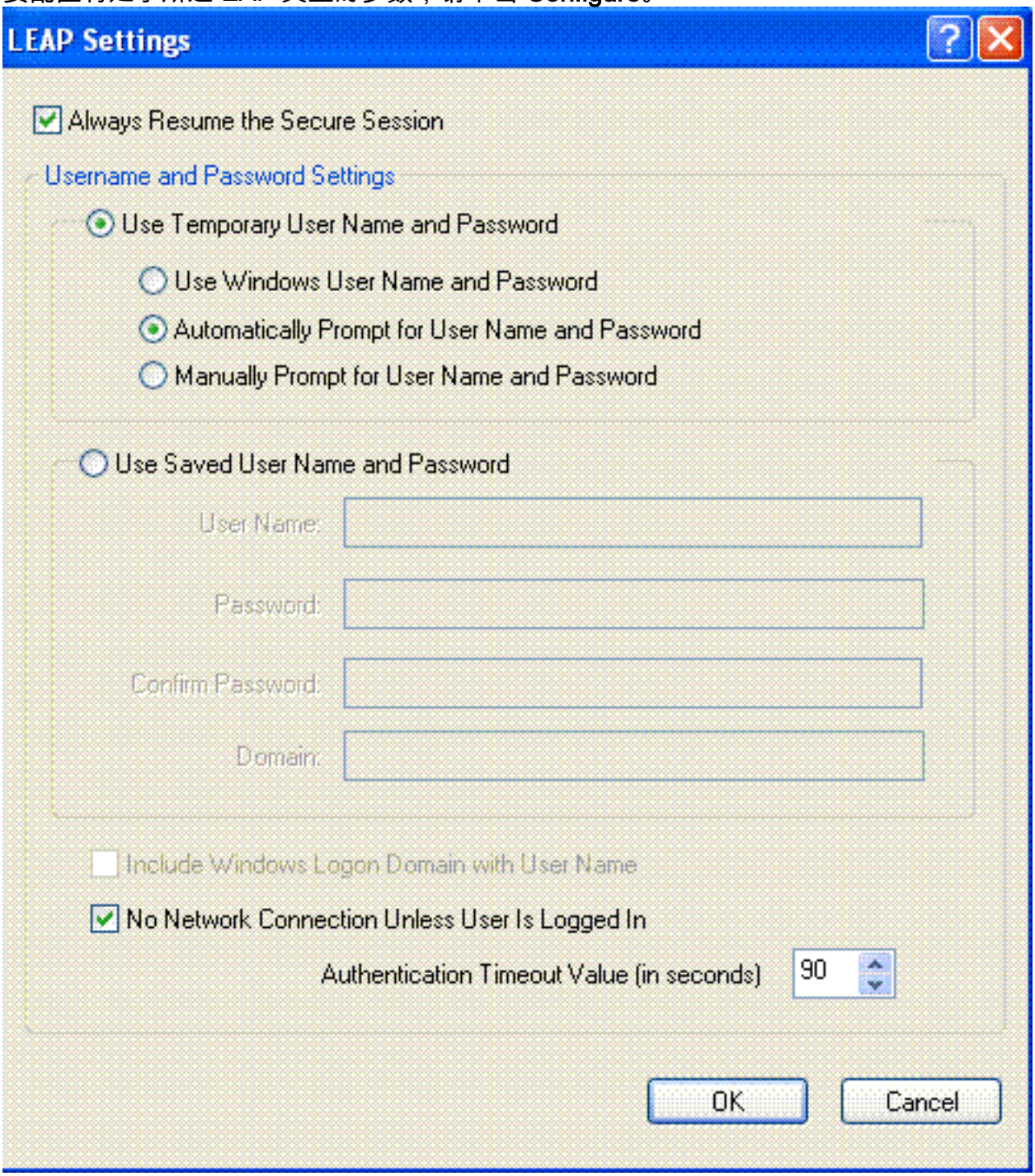


4. 单击 **Security** 选项卡。

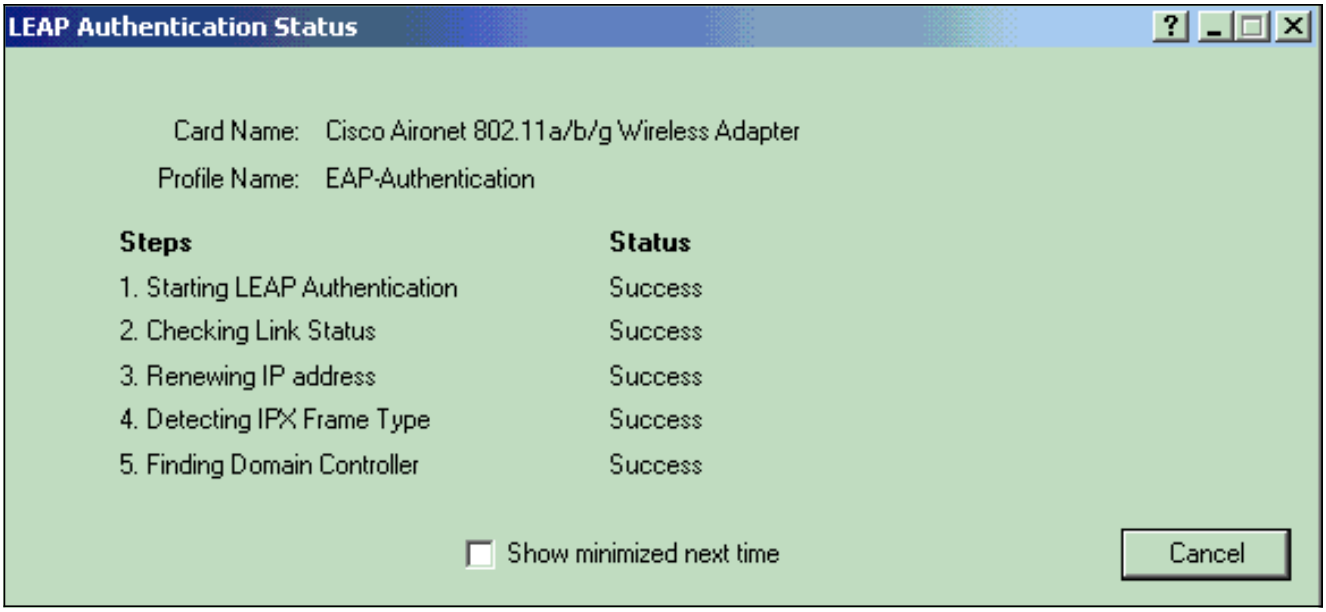


5. 点击**802.1x**单选按钮。

6. 从802.1x EAP请键入下拉列表，选择使用的EAP类型。
7. 要配置特定于所选 EAP 类型的参数，请单击 **Configure**。

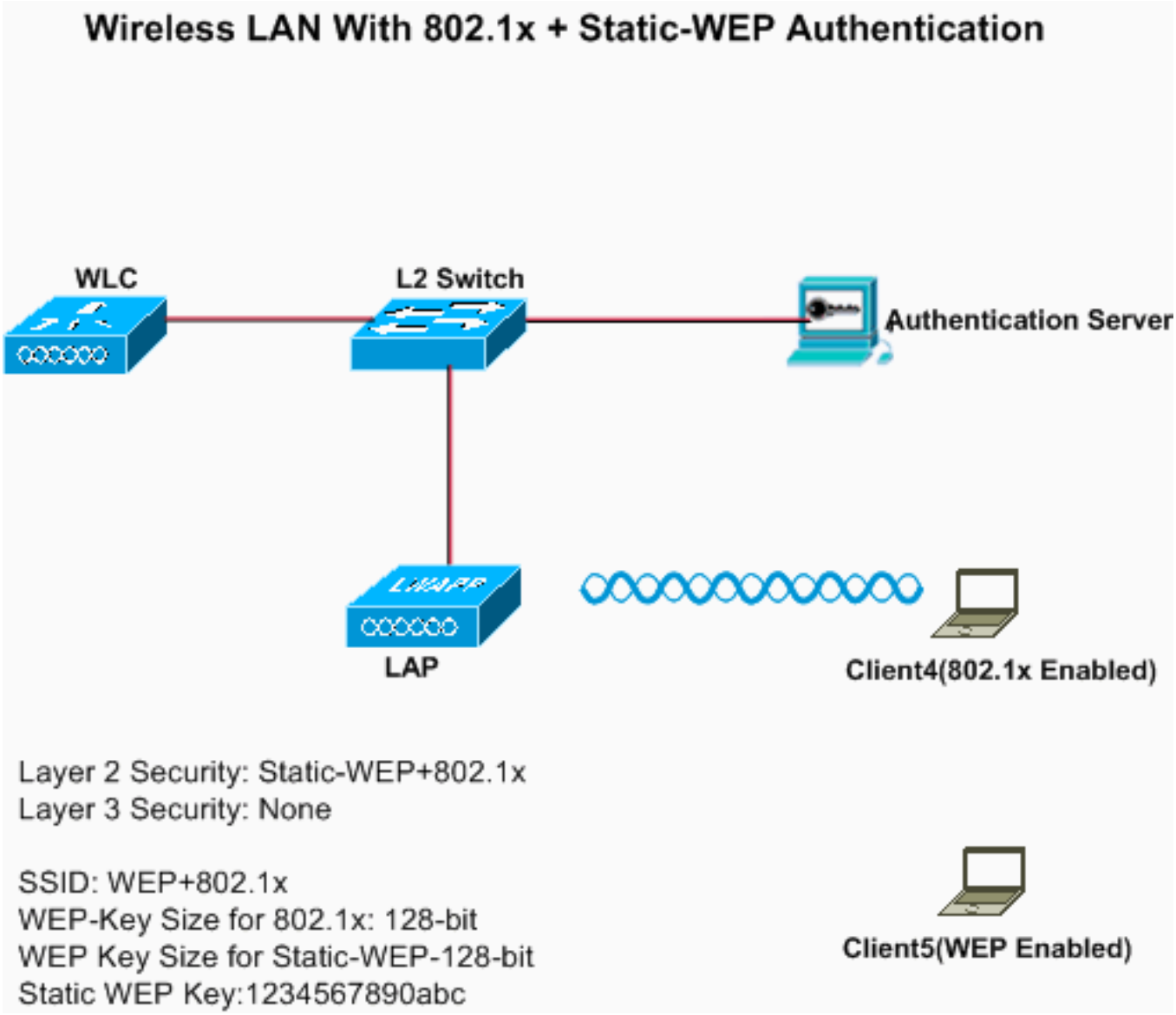


8. 单击 **Apply**。激活 SSID 后，无线客户端将使用 802.1x 身份验证连接到 WLAN。动态WEP密钥使用会话。



静态 WEP + 802.1x 身份验证

此示例显示一WLAN配置有静态WEP + 802.1x认证。



要配置 WLC 使用该设置，请完成以下步骤：

1. 要创建 WLAN，请从控制器 GUI 中单击 **WLANs**。随即显示 WLAN 窗口。该窗口列出了控制器中配置的 WLAN。
2. 要配置新的 WLAN，请单击 **New**。
3. 输入 WLAN ID 和 WLAN SSID。在本例中， WLAN被命名*WEP+802.1x*，并且WLAN ID是*4*。

4. 单击 **Apply**。
5. 在“WLAN”>“Edit”窗口中，定义特定于该 WLAN 的参数。从第2层下拉列表，请选择**Static-WEP+802.1x**。这将为该 WLAN 启用静态 WEP 和 802.1x 身份验证。使用802.1x，如前一个示例所显示，在RADIUS服务器参数下，请选择将使用验证客户机证书的RADIUS服务器，并且配置RADIUS服务器。如前一个镜像所显示，在静态WEP参数下，请选择WEP密钥大小和主索引，并且输入静态WEP加密密钥。选择根据您的设计需求的其他参数。此示例使用默认值。

配置无线客户端使用静态 WEP 和 802.1x

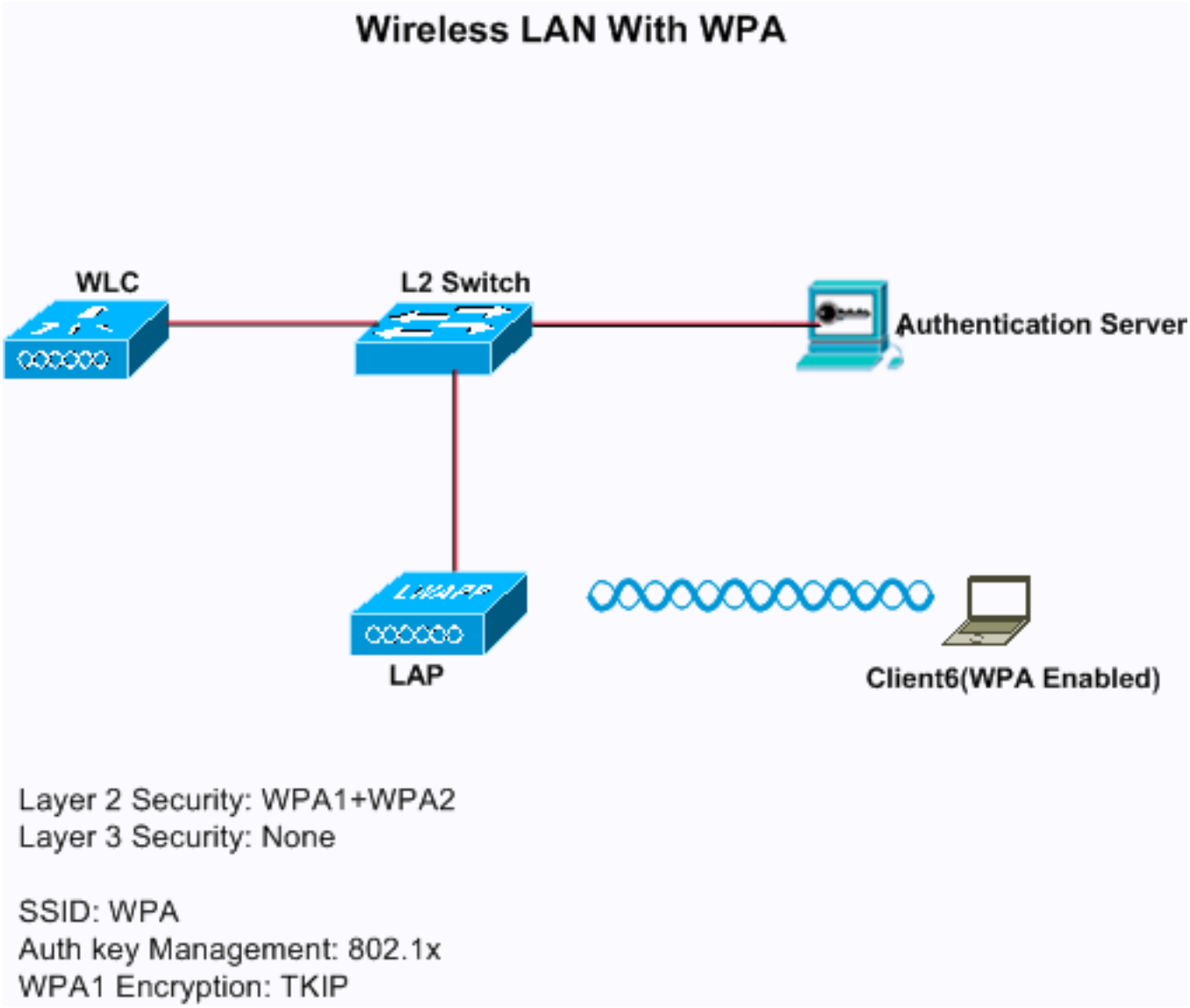
有关如何配置无线客户端的信息，请参阅配置无线客户端使用 802.1x 身份验证和配置无线客户端使用静态 WEP 部分。

一旦客户端配置文件被创建，为静态WEP关联被配置用LAP的客户端。要连接到网络，请使用 SSID WEP+802.1x。

同样，配置为使用 802.1x 身份验证的无线客户端将使用 EAP 进行身份验证并使用同一 SSID WEP+802.1x 访问网络。

Wi-Fi 保护访问

本示例说明了配置为使用 WPA 的 WLAN，而该 WPA 使用 802.1x。

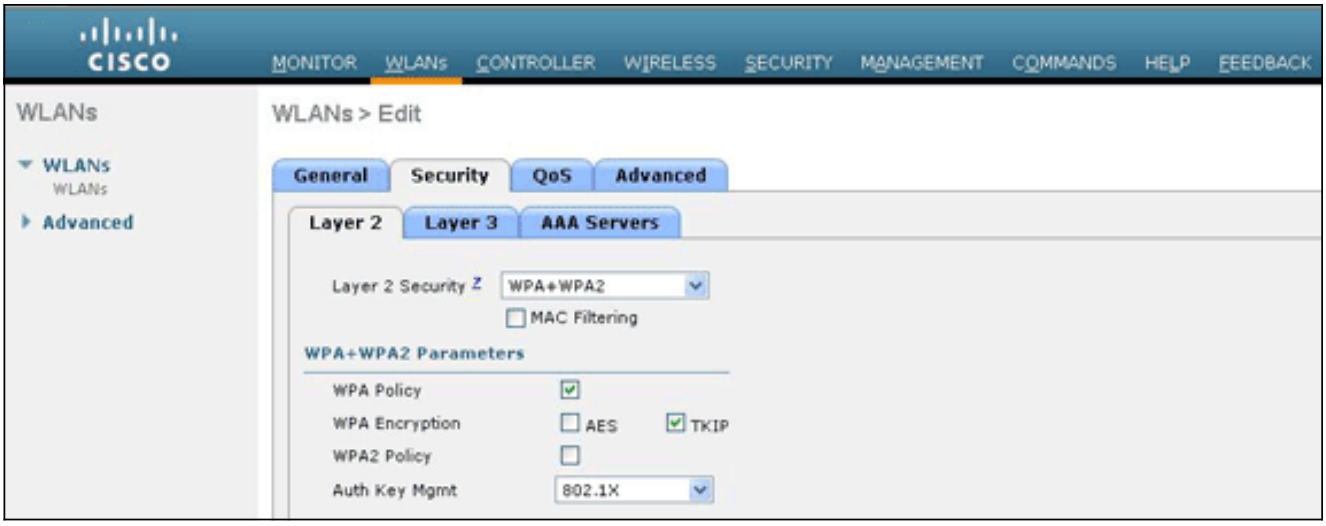


配置 WLC 使用 WPA

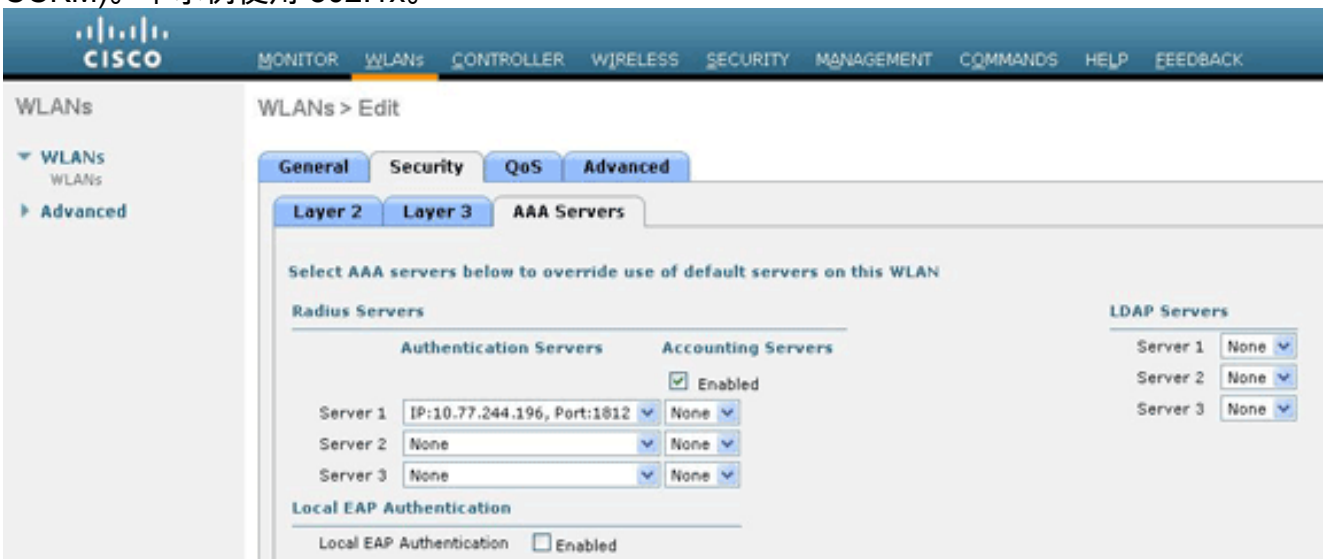
要配置 WLC 使用该设置，请完成以下步骤：

1. 要创建 WLAN，请从控制器 GUI 中单击 **WLANs**。随即显示 WLAN 窗口。该窗口列出了控制器中配置的 WLAN。
2. 点击**去**为了配置一新的WLAN。选择类型和配置文件名字。在本例中， WLAN被命名 *WPA*，并且WLAN ID是*5*。

3. 单击 **Apply**。
4. 在“WLAN”>“Edit”窗口中，定义特定于该 WLAN 的参数。



点击**安全**选项，点击第**2层**选项，并且从第2层安全下拉列表选择**WPA1+WPA2**。在“WPA1+WPA2 Parameters”下，选中 **WPA1 Policy** 复选框以启用 WPA1，选中“WPA2 Policy”复选框以启用 WPA2，或同时选中这两个复选框以同时启用 WPA1 和 WPA2。对 WPA1 和 WPA2 禁用默认值。如果留下WPA1和WPA2被禁用，接入点在他们的引导和探测响应信息要素仅做通告为您选择的认证密钥管理方法。选中 **AES** 复选框以启用 AES 数据加密，或选中“TKIP”复选框以对 WPA1、WPA2（或二者）启用 TKIP 数据加密。WPA1 和 WPA2 的默认值分别为 TKIP 和 AES。从Auth键Mgmt下拉列表选择这些密钥管理方法之一：*802.1X*—如果选择此选项，只有支持802.1x客户端。*CCKM*—如果选择此选项，只有支持CCKM客户端，其中客户端处理到认证的一个外部服务器。*PSK*—如果选择此选项，预共享密钥使用WLC和客户端。并且，规定所有标准用于在预标准前;例如， WPA/WPA2采取在CCKM的先例，当同时使用。*802.1X+CCKM*—如果选择此选项，支持CCKM或非CCKM客户端(可选的CCKM)。本示例使用 802.1x。



Note: 如果选择PSK，从PSK格式下拉列表请选择**ascii**或**十六进制**，在空白字段然后输入预共享密钥。WPA预共享密钥必须包含8个到63个ASCII文本字符或64个六角形的字符。

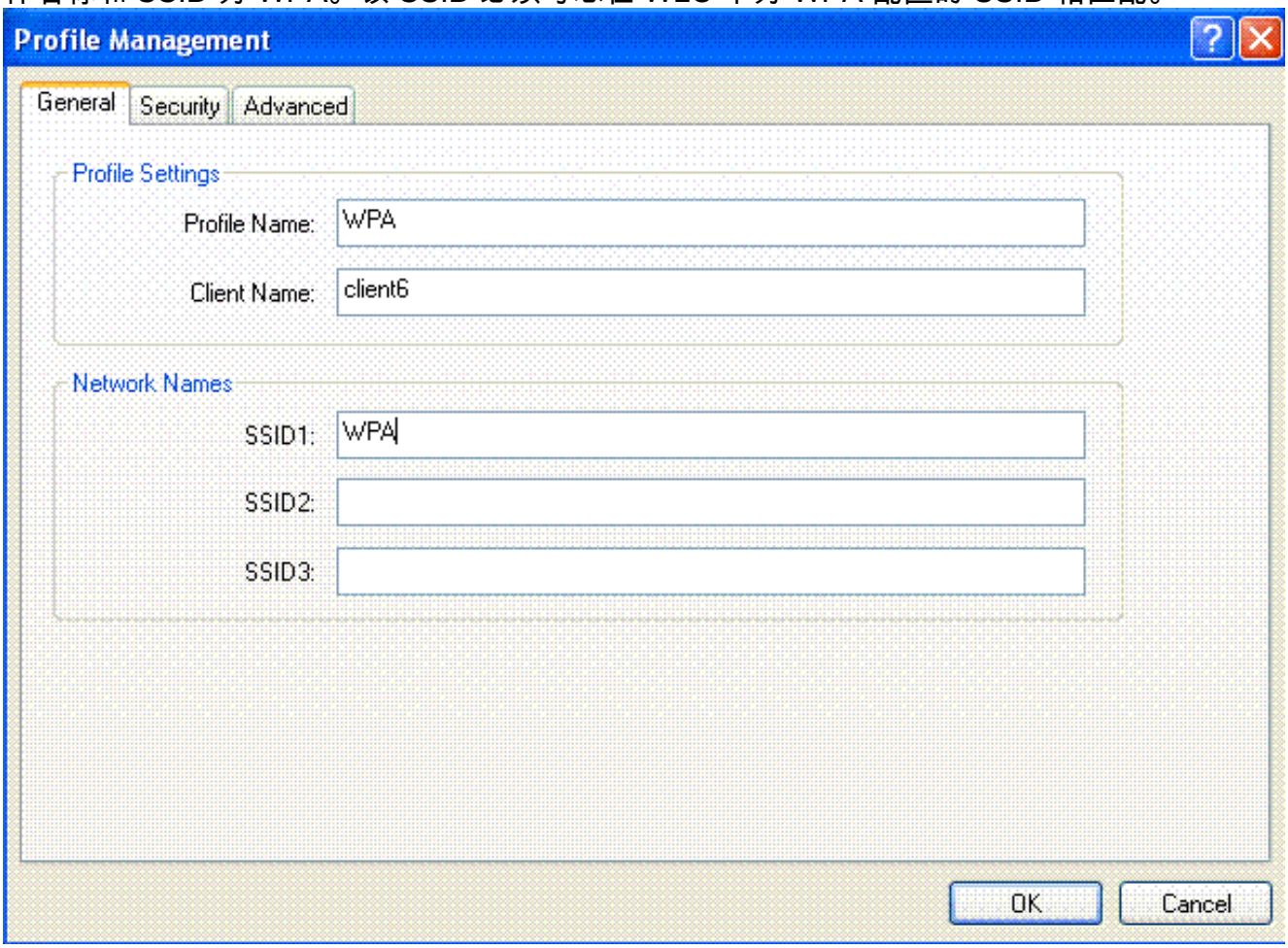
5. 点击**适用**为了应用您的更改。

配置无线客户端使用 WPA

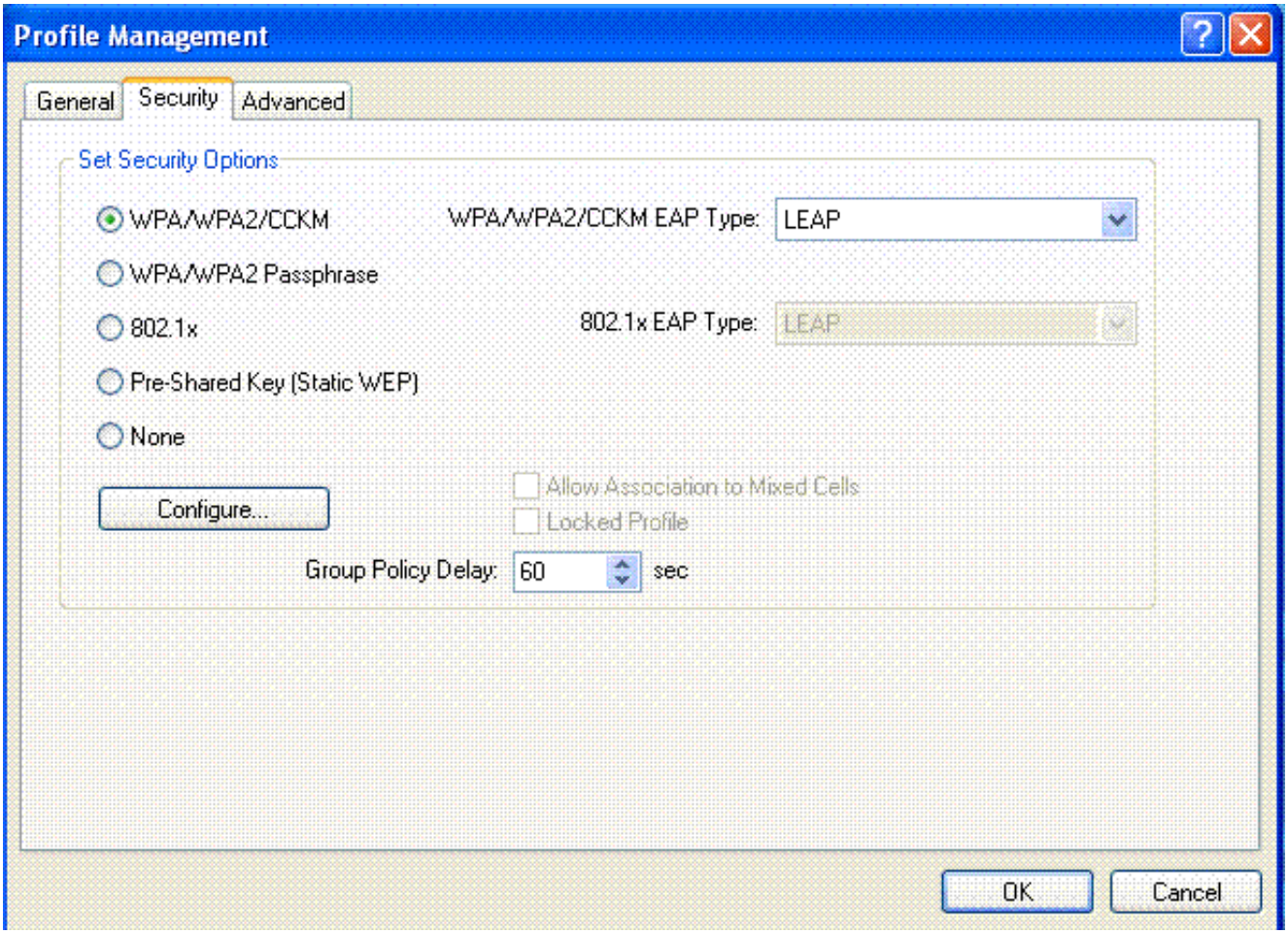
完成这些步骤为了配置此设置的无线局域网客户端：

1. 在 ADU 上的“Profile Management”窗口中，单击 **New** 以创建一个新配置文件。
2. 点击**一般**选项，并且输入客户端适配器将使用的配置文件名字和SSID。在本示例中，配置文

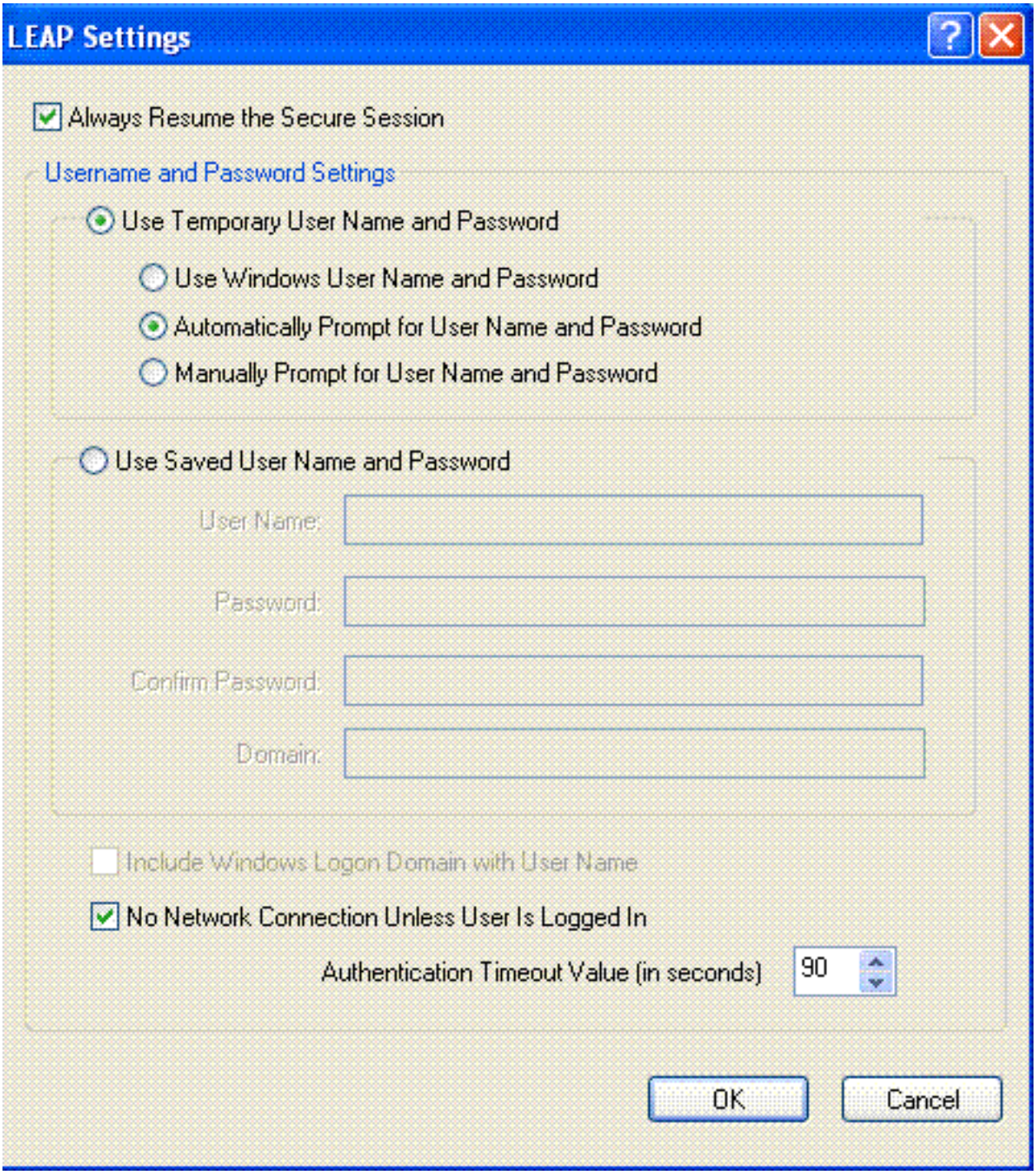
件名称和 SSID 为 WPA。该 SSID 必须与您在 WLC 中为 WPA 配置的 SSID 相匹配。



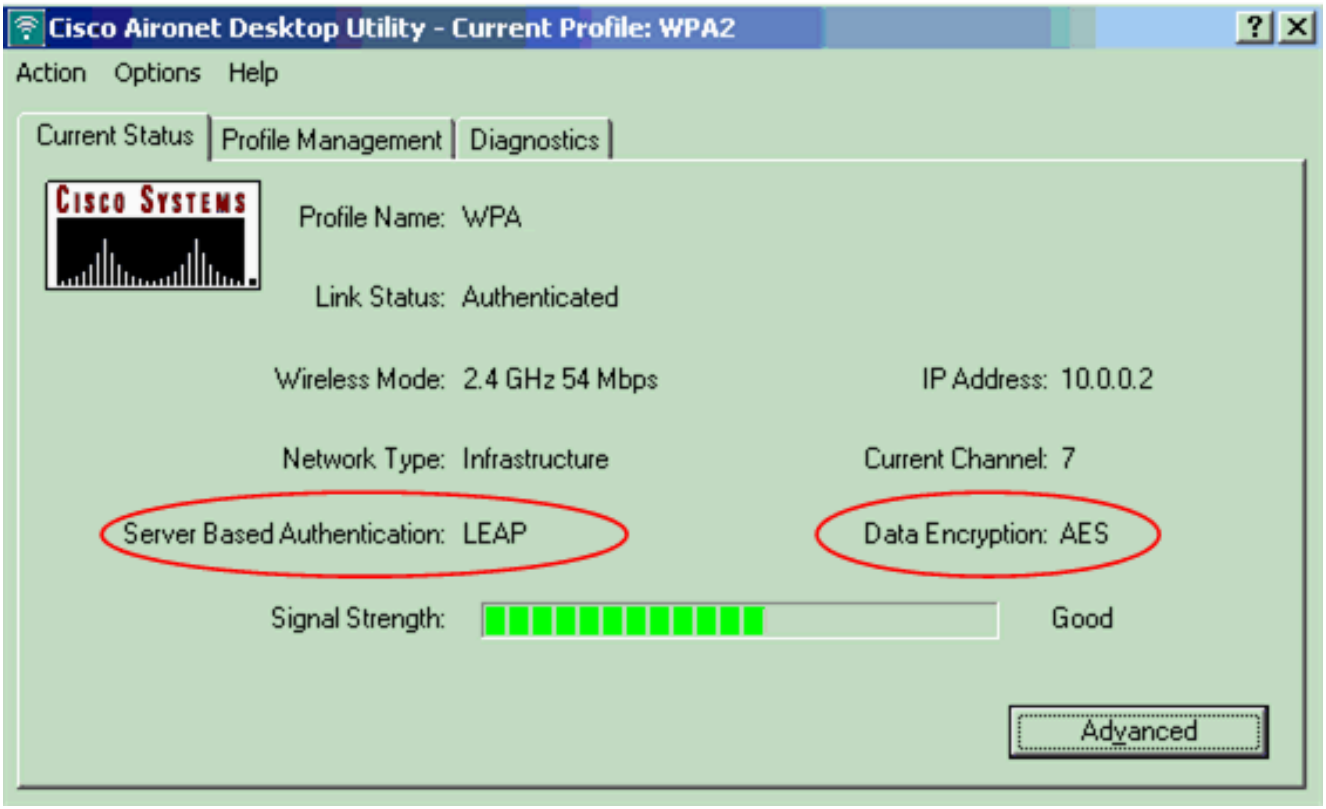
3. 在安全选项，请点击**WPA/WPA2/CCKM**单选按钮，并且从WPA/WPA2/CCKM EAP类型下拉列表选择适当的EAP类型。此步骤enable (event) WPA。



4. 单击 **Configure** 以定义特定于所选 EAP 类型的 EAP 设置。

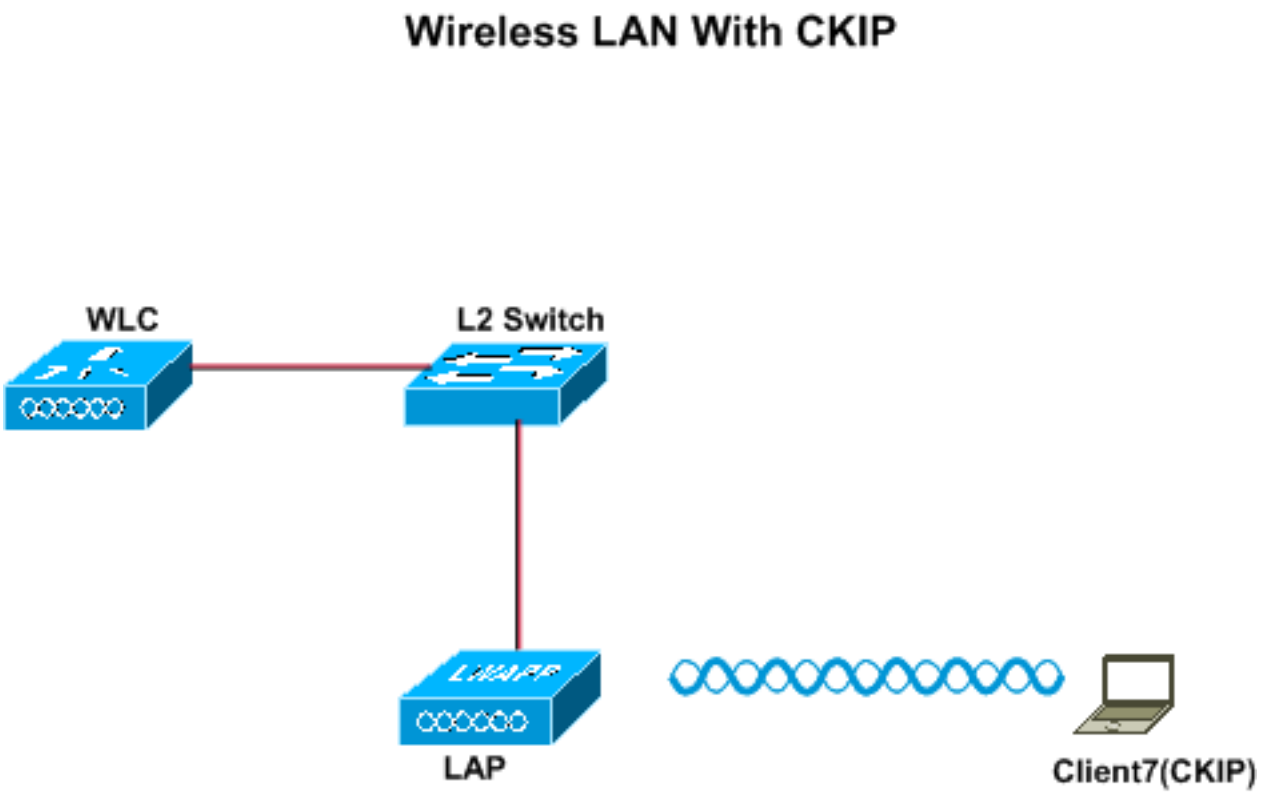


5. 单击 **Ok**。**Note:** 激活此配置文件后，将使用 802.1x 对客户端进行身份验证，并且在身份验证成功后，客户端将连接到 WLAN。检查 ADU 当前状态以确认客户端使用 TKIP 加密（WPA1 所使用的默认加密）和 EAP 身份验证。



CKIP

此示例显示一WLAN配置有CKIP。



Layer 2 Security: CKIP
Layer 3 Security: None
SSID: CKIP

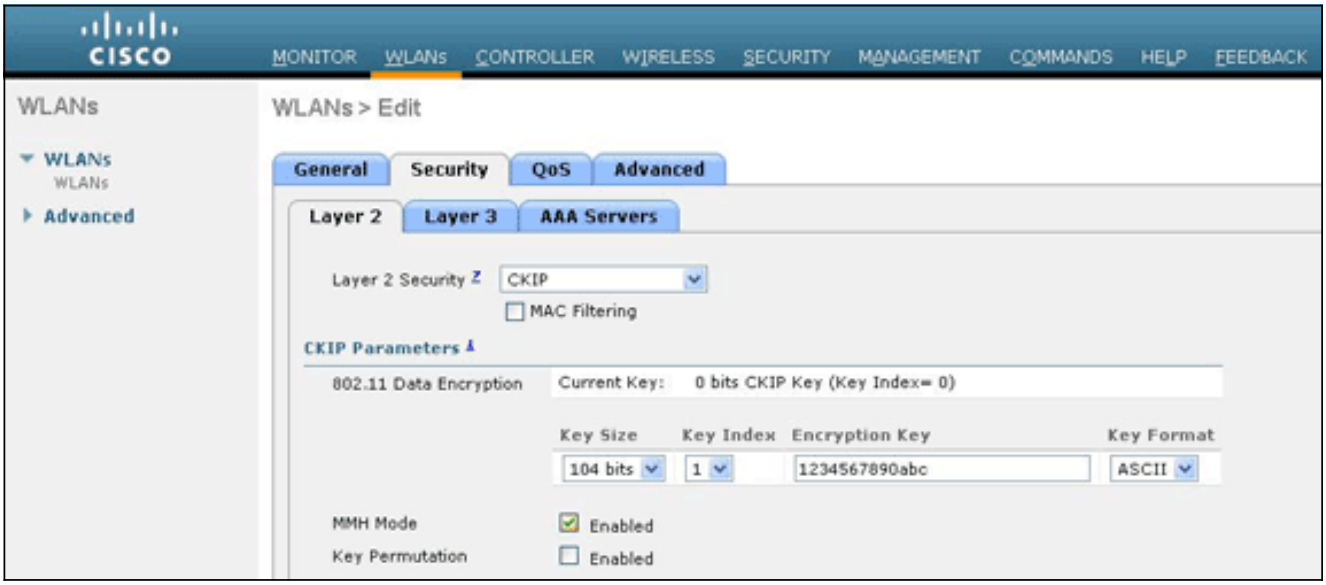
配置 WLC 使用 CKIP

要配置 WLC 使用该设置，请完成以下步骤：

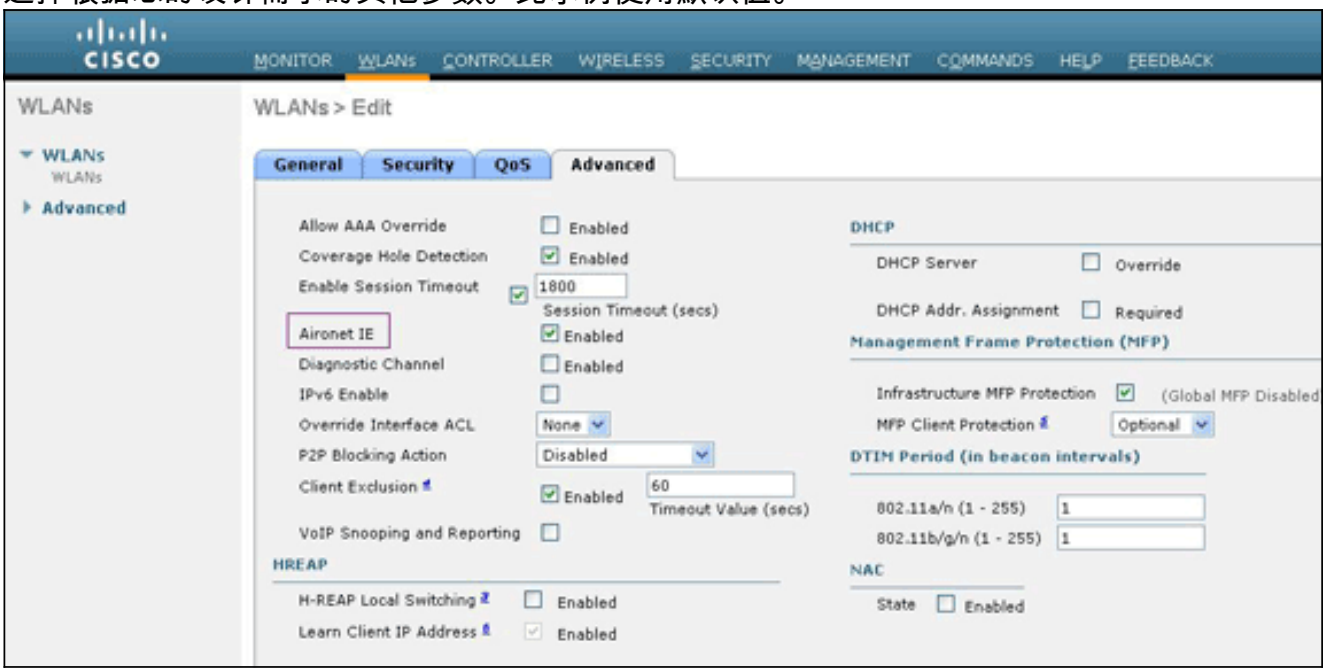
1. 要创建 WLAN，请从控制器 GUI 中单击 **WLANs**。随即显示 WLAN 窗口。该窗口列出了控制器中配置的 WLAN。
2. 要配置新的 WLAN，请单击 **New**。选择类型和配置文件名字。在本示例中，WLAN 的名称为 CKIP，WLAN ID 为 6。

3. 在“WLAN”>“Edit”窗口中，定义特定于该 WLAN 的参数。从第2层下拉列表，请选择**CKIP**。此WLAN的此步骤enable (event) CKIP。在CKIP参数下，请选择密钥大小和主索引，并且输入静态加密密钥。密钥大小可以是40位、104位或者128位。密钥索引可以介于 1 和 4 之间。一个唯一WEP密钥索引可以被运用于每WLAN。由于只有四个WEP密钥索引，只有四WLANs可以为静态WEP第2层加密被配置。对于CKIP，请选择**MMH模式**选项或者**关键置换**选项或者两个

。**Note:** 为使 CKIP 按预期工作，必须选择这两个参数之一或同时选择二者。如果未选择这两个参数，WLAN 将保持处于禁用状态。在本例中， 104使用关键的位，并且键是1234567890abc。



4. 选择根据您的设计需求的其他参数。此示例使用默认值。

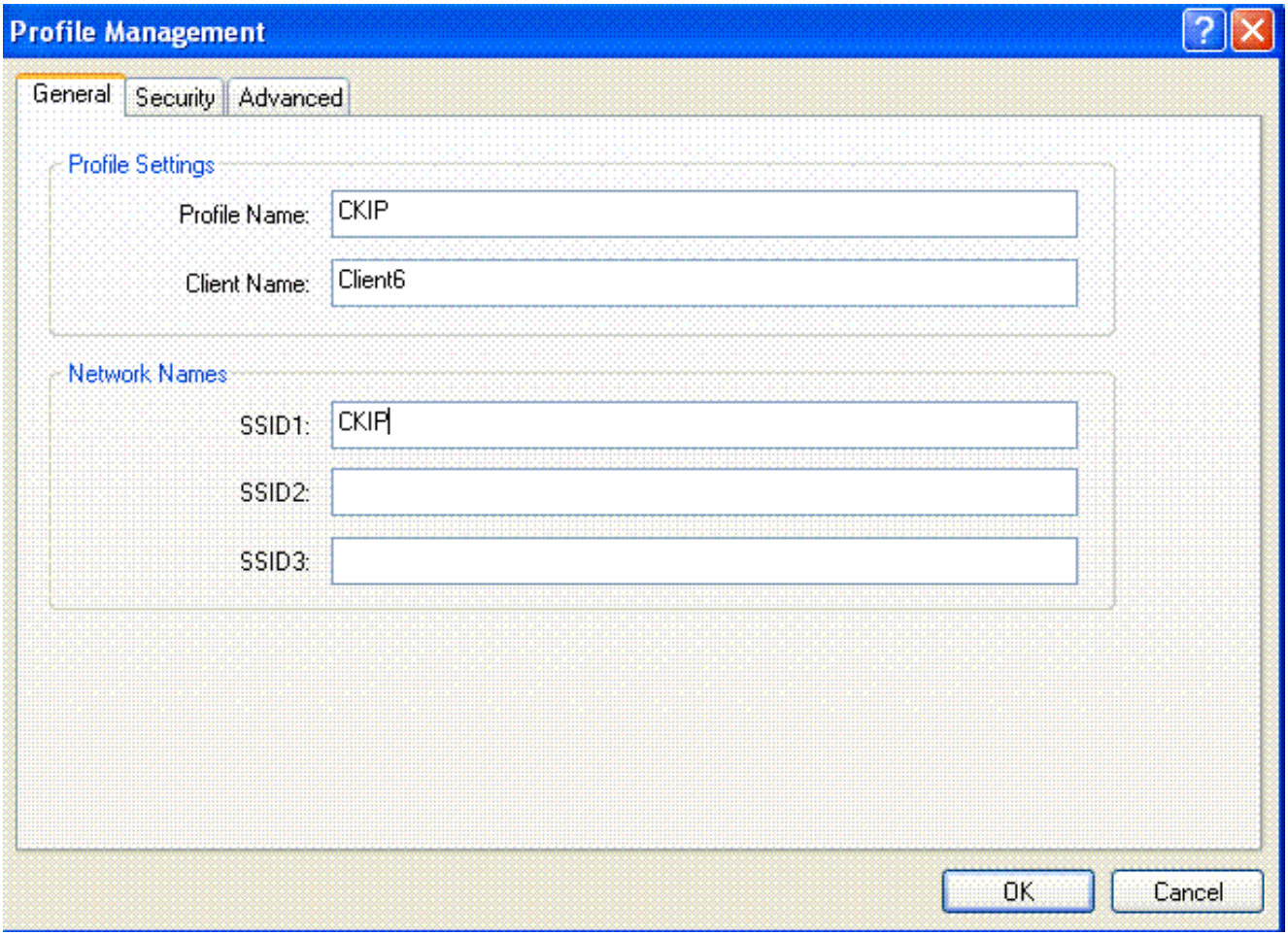


5. 单击 **Apply**。**Note:** CKIP 对 1100、1130 和 1200 AP 有效，但对 AP1000 无效。要使此功能正常运行，需要启用 Aironet IE。CKIP 将加密密钥扩展到 16 字节。

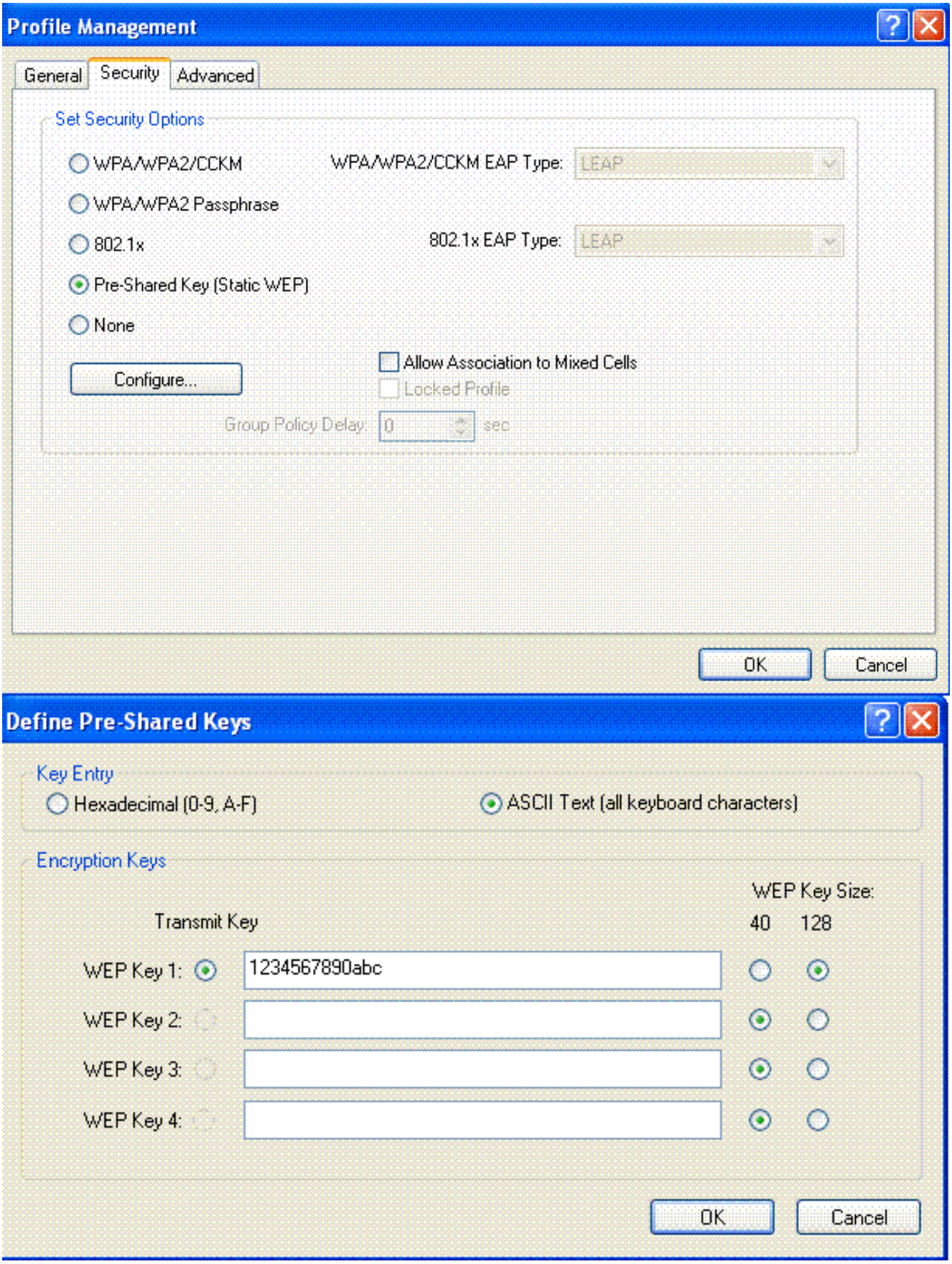
配置无线客户端使用 CKIP

要配置无线 LAN 客户端使用该设置，请完成以下步骤：

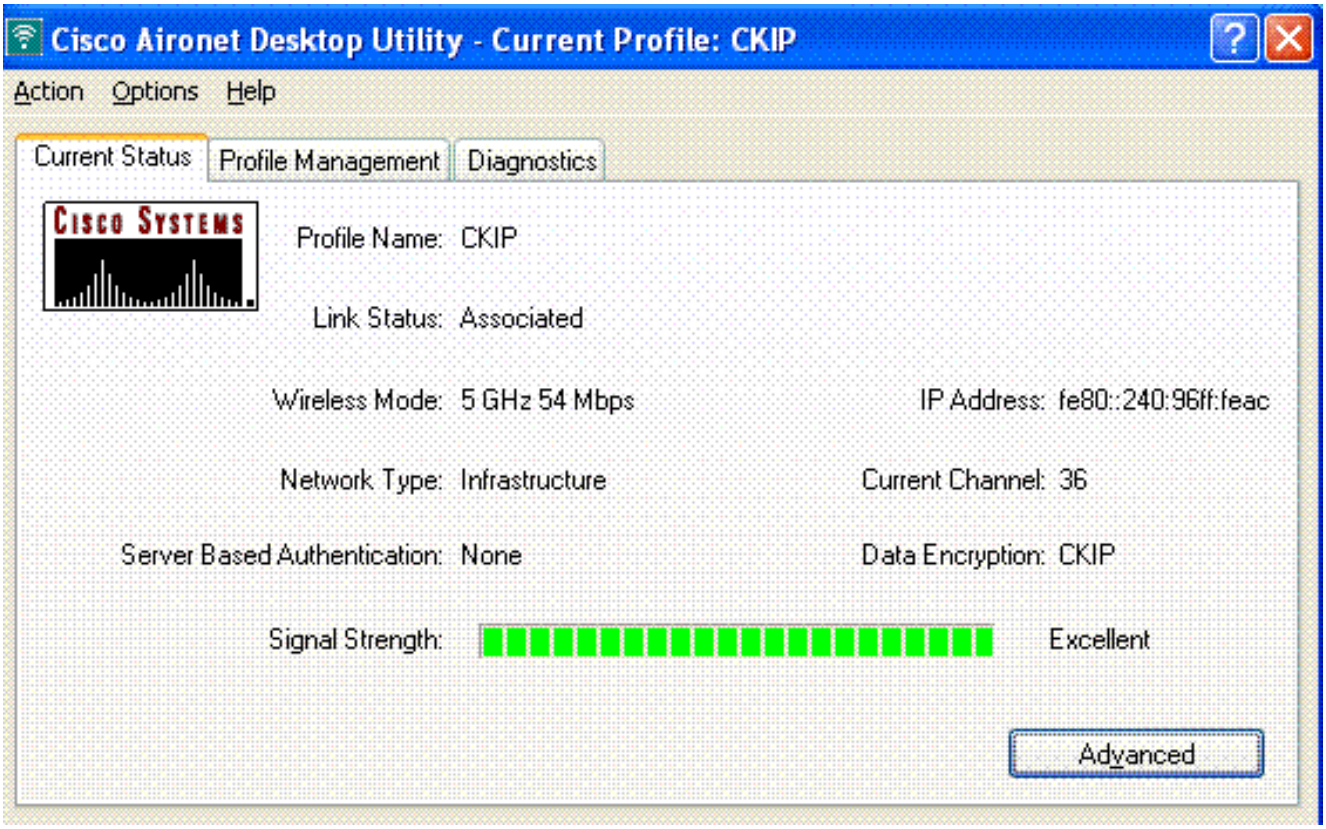
1. 为了创建新配置文件，请点击在ADU的**配置文件管理**选项，然后点击**新**。
2. 当配置文件管理(一般)时窗口显示，请完成这些步骤为了设置配置文件名字、客户端名和SSID：在“Profile Name”字段中输入配置文件的名称。此示例使用*CKIP*作为配置文件名字。在“Client Name”字段中输入客户端的名称。客户端名称用于标识 WLAN 网络中的无线客户端。此配置使用*Client6*客户端名。在“Network Names”下，输入用于该配置文件的 SSID。该 SSID 与您在 WLC 中配置的 SSID 相同。本示例中的 SSID 为 CKIP。



3. 单击 **Security** 选项卡。
4. 选择**预共享密钥(静态WEP)**在集安全选项下，点击**配置**，并且定义了WEP密钥大小和WEP密钥。这些值应该与在此WLAN的WLC配置的WEP密钥配比。



5. 单击 **Ok**。激活 SSID 后，无线客户端将与 LAP 和 WLC 协商使用 CKIP 加密数据包。



第 3 层安全解决方案

Web 策略（Web 身份验证和 Web 传递）

如何的信息参考无线局域网控制器Web身份验证配置示例关于对enable (event)在WLAN网络的Web认证。

关于如何配置外部Web认证和Web转接认证的信息在WLAN，参考与无线局域网控制器配置示例的外部Web认证。

如何的更多信息参考无线局域网控制器Web转接配置示例关于对enable (event)在WLAN网络的Web转接。

飞溅页机制是在WLC版本5.0引入的第3层安全机制用于客户端验证。参考无线局域网控制器飞溅页重定向配置示例欲知更多信息。

VPN 传递

有关如何在 WLAN 中配置 VPN 传递的信息，请参阅 WLC 中通过无线 LAN 的客户端 VPN 的配置示例。

Troubleshoot

故障排除命令

您能使用这些调试指令排除您的配置故障。

Web 身份验证的调试：

- **debug mac addr <client-MAC-address xx:***xx* **：***xx* **：***xx* **：***xx* **：***xx***>** — 配置客户端的 MAC 地址调试。
- **debug aaa all enable** — 配置所有 AAA 消息的调试。
- **debug pem state enable** — 配置策略管理器状态机的调试。
- **debug pem events enable** — 配置策略管理器事件的调试。
- **debug dhcp message enable** — 使用此命令以显示有关动态主机配置协议 (DHCP) 客户端活动的调试信息并监控 DHCP 数据包的状态。
- **debug dhcp packet enable** — 使用此命令以显示 DHCP 数据包级别信息。
- **debug pm ssh-appgw enable** — 配置应用程序网关的调试。
- **debug pm ssh-tcp enable** — 配置策略管理器 tcp 处理的调试。

WEP 的调试：不对 WEP 进行调试，因为 WEP 是在 AP 中执行的，请打开 **debug dot11 all enable**。

802.1X/WPA/RSN/PMK 缓存的调试：

- **debug mac addr <client-MAC-address xx:***xx* **：***xx* **：***xx* **：***xx* **：***xx***>** — 配置客户端的 MAC 地址调试。
- **debug dot1x all enable** — 使用此命令以显示 802.1X 调试信息。
- **debug dot11 all enable** — 使用此命令以启用无线电功能的调试。
- **debug pem events enable** — 配置策略管理器事件的调试。
- **debug pem state enable** — 配置策略管理器状态机的调试。
- **debug dhcp message enable** — 使用此命令以显示有关动态主机配置协议 (DHCP) 客户端活动的调试信息并监控 DHCP 数据包的状态。
- **debug dhcp packet enable** — 使用此命令以显示 DHCP 数据包级别信息。
- **debug mobility handoff enable (针对交换机内漫游)** — 配置移动数据包的调试。
- **show client detail <mac>** — 按 MAC 地址显示客户端的详细信息。检查 WLAN 和 RADIUS 会话超时配置。

Related Information

- 根据 WLC 和 Cisco Secure ACS 的 SSID 限制 WLAN 访问的配置示例
- 无线 LAN 控制器中的 ACL 配置示例
- Cisco 无线 LAN 控制器配置指南 4.0 版
- 无线支持页
- Technical Support & Documentation - Cisco Systems