在固定 ISR 上配置无线身份验证类型

目录

简介
先决条件
要求
使用的组件
规则
背景信息
配置
网络图
配置开放式身份验证
配置集成路由和桥接(IRB)并设置网桥组
配置桥接虚拟接口(BVI)
配置开放式身份验证的SSID
为此VLAN的无线客户端配置内部DHCP服务器
配置802.1x/EAP身份验证
配置集成路由和桥接(IRB)并设置网桥组
配置桥接虚拟接口(BVI)
为EAP身份验证配置本地RADIUS服务器
配置802.1x/EAP身份验证的SSID
为此VLAN的无线客户端配置内部DHCP服务器
WPA密钥管理
配置WPA-PSK
配置集成路由和桥接(IRB)并设置网桥组
配置桥接虚拟接口(BVI)
为WPA-PSK身份验证配置SSID
为此VLAN的无线客户端配置内部DHCP服务器
配置WPA（使用EAP）身份验证
配置集成路由和桥接(IRB)并设置网桥组
配置桥接虚拟接口(BVI)
为WPA身份验证配置本地RADIUS服务器
为采用EAP身份验证的WPA配置SSID
为此VLAN的无线客户端配置内部DHCP服务器
配置无线客户端进行身份验证
配置无线客户端进行开放式身份验证
配置无线客户端进行802.1x/EAP身份验证
配置无线客户端进行WPA-PSK身份验证
为WPA（采用EAP）身份验证配置无线客户端
故障排除
故障排除命令
相关信息

简介

本文档提供说明如何在思科无线集成固定配置路由器上配置各种第 2 层身份验证类型，以使用 CLI 命令实现无线连接的配置示例。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 了解如何配置思科集成多业务路由器(ISR)的基本参数
- 了解如何使用Aironet桌面实用程序(ADU)配置802.11a/b/g无线客户端适配器

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Cisco IOS®软件版本12.3(8)YI1的Cisco 877W ISR
- 带Aironet台式机实用程序的笔记本电脑版本3.6
- 运行固件版本3.6的802.11 a/b/g客户端适配器

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

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

思科集成多业务固定配置路由器支持安全、经济且易于使用的无线局域网解决方案，该解决方案将移动性和灵活性与网络专业人员所需的企业级功能相结合。使用基于Cisco IOS软件的管理系统，Cisco路由器充当接入点，并且是Wi-Fi认证的、符合IEEE 802.11a/b/g标准的无线LAN收发器。

您可以使用命令行界面(CLI)、基于浏览器的管理系统或简单网络管理协议(SNMP)配置和监控路由器。本文档介绍如何使用CLI命令配置ISR以实现无线连接。

配置

本示例显示如何使用CLI命令在思科无线集成固定配置路由器上配置这些身份验证类型。

- 开放式身份验证

- 802.1x/EAP（可扩展身份验证协议）身份验证
- Wi-Fi保护访问预共享密钥(WPA-PSK)身份验证
- WPA（使用EAP）身份验证

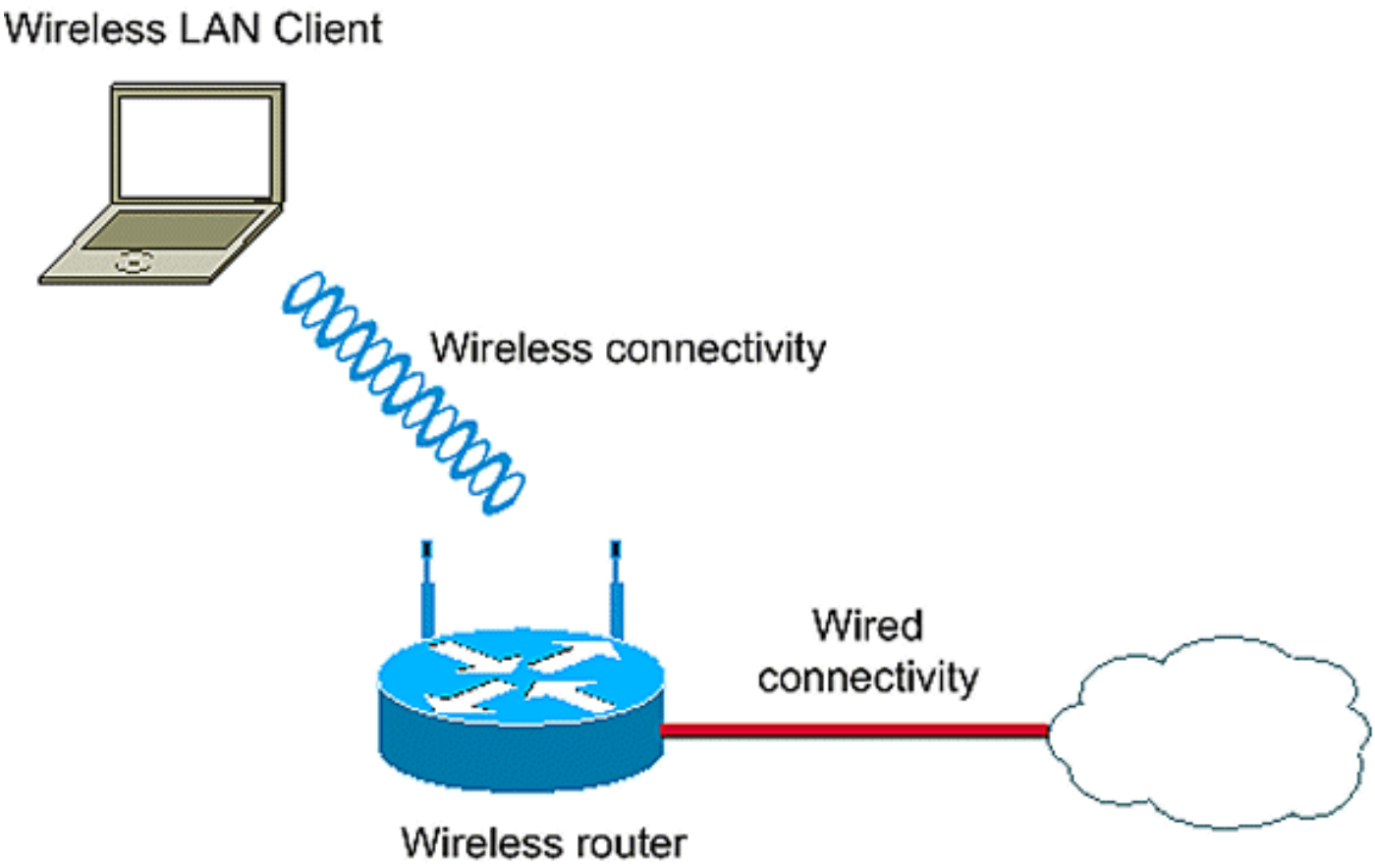
注意：本文档不关注共享身份验证，因为它是安全性较低的身份验证类型。

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）。

网络图

本文档使用以下网络设置：



此设置使用无线ISR上的本地RADIUS服务器通过802.1x身份验证对无线客户端进行身份验证。

配置开放式身份验证

开放式身份验证是空的身份验证算法。接入点会授予任何身份验证请求。开放式身份验证允许任何设备访问网络。如果网络上未启用加密，任何知道接入点SSID的设备都可以访问网络。在接入点上启用WEP加密后，WEP密钥本身就成为一种访问控制手段。如果设备没有正确的WEP密钥，即使身份验证成功，设备仍无法通过接入点传输数据。它也不能解密从接入点发送的数据。

本示例配置仅介绍简单的开放式身份验证。WEP密钥可以设为强制或可选。此示例将WEP密钥配置

为可选密钥，这样任何不使用WEP的设备也可以验证并与此AP关联。

有关详细信息，请参阅开放式身份验证。

此示例使用此配置设置在ISR上配置开放式身份验证。

- SSID名称：“open”
- VLAN 1
- 内部DHCP服务器范围:10.1.0.0/16

注意：为了简单起见，本示例不对经过身份验证的客户端使用任何加密技术。

在路由器上完成以下操作：

1. 配置集成路由和桥接(IRB)并设置网桥组
2. 配置桥接虚拟接口(BVI)
3. 配置开放式身份验证的SSID
4. 为此VLAN的无线客户端配置内部DHCP服务器

配置集成路由和桥接(IRB)并设置网桥组

完成以下操作：

1. 在路由器中启用IRB。

   router<configure>#bridge irb

   注：如果所有安全类型都要在单个路由器上配置，则仅可在路由器上全局启用一次IRB就足够了。不需要为每个单独的身份验证类型启用它。

2. 定义网桥组。

   本示例使用网桥组编号 1。

   router<configure>#bridge 1

3. 选择网桥组的生成树协议。

   此处，为此网桥组配置了IEEE生成树协议。

   router<configure>#bridge 1 protocol ieee

4. 使 BVI 从其对应的网桥组接受和路由可路由的数据包。

   此示例使BVI能够接受和路由IP数据包。

   router<configure>#bridge 1 route ip

配置桥接虚拟接口(BVI)

完成以下操作：

1. 配置BVI。

   将网桥组的相应号码分配给BVI时配置BVI。每个网桥组只能有一个对应的BVI。在本例中，将网桥组编号 1 分配给 BVI。

   router<configure>#interface BVI <1>

2. 为BVI分配IP地址。

   router<config-if>#ip address 10.1.1.1 255.255.0.0

   router<config-if>#no shut

有关桥接的详细信息，请参阅配置桥接。

配置开放式身份验证的SSID

完成以下操作：

1. 启用无线电接口

   要启用无线电接口，请转到DOT11无线电接口配置模式并为接口分配SSID。

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid open

   开放式身份验证类型可以与MAC地址身份验证结合配置。在这种情况下，接入点会强制所有客户端设备执行MAC地址身份验证，然后才允许它们加入网络。

   开放式身份验证也可与EAP身份验证一起配置。接入点会强制所有客户端设备执行EAP身份验证，然后才允许它们加入网络。对于list-name，指定身份验证方法列表。

   为EAP身份验证配置的接入点强制所有关联客户端设备执行EAP身份验证。未使用EAP的客户端设备无法使用接入点。

2. 将SSID绑定到VLAN。

   要在此接口上启用SSID，请在SSID配置模式下将SSID绑定到VLAN。

   router<config-ssid>vlan 1

3. 使用开放式身份验证配置SSID。

   router<config-ssid>#authentication open

4. 为WEP密钥配置无线电接口（可选）。

   router<config>#encryption vlan 1 mode WEP optional

5. 在无线电接口上启用VLAN。

   router<config>#interface Dot11Radio 0.1

   router<config-subif>#encapsulation dot1Q 1

   router<config-subif>#bridge-group 1

为此VLAN的无线客户端配置内部DHCP服务器

在全局配置模式下键入以下命令，配置此VLAN无线客户端的内部DHCP服务器：

- ip dhcp excluded-address 10.1.1.1 10.1.1.5
- ip dhcp pool open

在DHCP池配置模式下，键入以下命令：

- network 10.1.0.0 255.255.0.0
- default-router 10.1.1.1

配置802.1x/EAP身份验证

此身份验证类型为您的无线网络提供最高级别的安全性。使用可扩展身份验证协议(EAP)与兼容EAP的RADIUS服务器进行交互，接入点可帮助无线客户端设备和RADIUS服务器执行相互身份验证并生成动态单播WEP密钥。RADIUS服务器将WEP密钥发送到接入点，接入点会将其用于发送到客户端或从客户端接收的所有单播数据信号。

有关详细信息，请参阅EAP身份验证。

本示例使用以下配置设置：

- SSID名称：leap
- VLAN 2
- 内部DHCP服务器范围:10.2.0.0/16

本示例使用LEAP身份验证作为验证无线客户端的机制。

注意：请参阅Cisco Secure ACS for Windows v3.2 With EAP-TLS Machine Authentication以配置EAP-TLS。

注意：请参阅使用PEAP-MS-CHAPv2计算机身份验证配置Cisco Secure ACS for Windows v3.2以配置PEAP-MS-CHAPv2。

注意：了解这些EAP类型的所有配置主要涉及客户端和身份验证服务器端的配置更改。对于所有这些身份验证类型，无线路由器或接入点上的配置或多或少保持不变。

注意：如最初所述，此设置使用无线ISR上的本地RADIUS服务器通过802.1x身份验证对无线客户端进行身份验证。

在路由器上完成以下操作：

1. 配置集成路由和桥接(IRB)并设置网桥组
2. 配置桥接虚拟接口(BVI)
3. 为EAP身份验证配置本地RADIUS服务器
4. 配置802.1x/EAP身份验证的SSID
5. 为此VLAN的无线客户端配置内部DHCP服务器

配置集成路由和桥接(IRB)并设置网桥组

完成以下操作：

1. 在路由器中启用IRB。

   router<configure>#bridge irb

   注：如果所有安全类型都要在单个路由器上配置，则仅可在路由器上全局启用一次IRB就足够了。不需要为每个单独的身份验证类型启用它。

2. 定义网桥组。

   本示例使用网桥组编号 2。

   router<configure>#bridge 2

3. 选择网桥组的生成树协议。

   此处，为此网桥组配置了IEEE生成树协议。

   router<configure>#bridge 2 protocol ieee

4. 选择网桥组的生成树协议。

   此处，为此网桥组配置了IEEE生成树协议。

   router<configure>#bridge 2 protocol ieee

5. 使BVI能够接受和路由从其相应网桥组接收的可路由数据包。

   此示例使BVI能够接受和路由IP数据包。

   router<configure>#bridge 2 route ip

配置桥接虚拟接口(BVI)

完成以下操作：

1. 配置BVI。

   将网桥组的相应号码分配给BVI时配置BVI。每个网桥组只能有一个对应的BVI。此示例将网桥组编号2分配给BVI。

   router<configure>#interface BVI <2>

2. 为BVI分配IP地址。

   router<config-if>#ip address 10.2.1.1 255.255.0.0

   router<config-if>#no shut

为EAP身份验证配置本地RADIUS服务器

如前所述，本文档使用无线感知路由器上的本地RADIUS服务器进行EAP身份验证。

1. 启用身份验证、授权和记帐(AAA)访问控制模型。

   router<configure>#aaa new-model

2. 为RADIUS服务器创建服务器组rad-eap。

   router<configure>#aaa group server radius rad-eap server 10.2.1.1 auth-port 1812 acct-port 1813

3. 创建方法列表eap_methods，列出用于验证AAA登录用户的身份验证方法。将方法列表分配给此服务器组。

   router<configure>#aaa authentication login eap_methods group rad-eap

4. 启用路由器作为本地身份验证服务器并进入身份验证器的配置模式。

   router<configure>#radius-server local

5. 在Radius服务器配置模式下，将路由器添加为本地身份验证服务器的AAA客户端。

   router<config-radsrv>#nas 10.2.1.1 key Cisco

6. 在本地Radius服务器上配置用户user1。

   router<config-radsrv>#user user1 password user1 group rad-eap

7. 指定RADIUS服务器主机。

   router<config-radsrv>#radius-server host 10.2.1.1 auth-port 1812 acct-port 1813 key

注意：此密钥应与nas命令中在radius-server配置模式下指定的密钥相同。

配置802.1x/EAP身份验证的SSID

802.1x/EAP的无线电接口和相关SSID的配置涉及路由器上各种无线参数的配置，包括SSID、加密模式和身份验证类型。本示例使用名为leap的SSID。

1. 启用无线电接口。

   要启用无线电接口，请转到DOT11无线电接口配置模式并为接口分配SSID。

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid leap

2. 将SSID绑定到VLAN。

   要在此接口上启用SSID，请在SSID配置模式下将SSID绑定到VLAN。

   router<config-ssid>#vlan 2

3. 使用802.1x/LEAP身份验证配置SSID。

   router<config-ssid>#authentication network-eap eap_methods

4. 配置用于动态密钥管理的无线电接口。

   router<config>#encryption vlan 2 mode ciphers wep40

5. 在无线电接口上启用VLAN。

   router<config>#interface Dot11Radio 0.2

   router<config-subif>#encapsulation dot1Q 2

   router<config-subif>#bridge-group 2

为此VLAN的无线客户端配置内部DHCP服务器

在全局配置模式下键入以下命令，配置此VLAN无线客户端的内部DHCP服务器：

- ip dhcp excluded-address 10.2.1.1 10.2.1.5
- ip dhcp pool leapauth

在DHCP池配置模式下，键入以下命令：

- network 10.2.0.0 255.255.0.0

- default-router 10.2.1.1

WPA密钥管理

Wi-Fi保护访问是基于标准的互操作性安全增强功能，可显着提高当前和未来无线LAN系统的数据保护和访问控制水平。

有关详细信息，请参阅WPA密钥管理。

WPA密钥管理支持两种互斥管理类型：WPA — 预共享密钥(WPA-PSK)和WPA（使用EAP）。

配置WPA-PSK

WPA-PSK用作无线LAN的密钥管理类型，其中基于802.1x的身份验证不可用。在此类网络中，必须在接入点上配置预共享密钥。您可以输入预共享密钥为ASCII或十六进制字符。如果以ASCII字符输入密钥，则输入8到63个字符，接入点将使用基于密码的加密标准(RFC2898)中所述的过程扩展密钥。如果输入密钥作为十六进制字符，则必须输入64个十六进制字符。

本示例使用以下配置设置：

- SSID名称：wpa-shared
- VLAN 3
- 内部DHCP服务器范围:10.3.0.0/16

在路由器上完成以下操作：

1. 配置集成路由和桥接(IRB)并设置网桥组
2. 配置桥接虚拟接口(BVI)
3. 为WPA-PSK身份验证配置SSID
4. 为此VLAN的无线客户端配置内部DHCP服务器

配置集成路由和桥接(IRB)并设置网桥组

完成以下操作：

1. 在路由器中启用IRB。

   router<configure>#bridge irb

   注：如果所有安全类型都要在单个路由器上配置，则仅可在路由器上全局启用一次IRB就足够了。不需要为每个单独的身份验证类型启用它。

2. 定义网桥组。

本示例使用网桥组编号 3。

router<configure>#bridge 3

3. 选择网桥组的生成树协议。

已为此网桥组配置IEEE生成树协议。

router<configure>#bridge 3 protocol ieee

4. 使 BVI 从其对应的网桥组接受和路由可路由的数据包。

此示例使BVI能够接受和路由IP数据包。

router<configure>#bridge 3 route ip

配置桥接虚拟接口(BVI)

完成以下操作：

1. 配置BVI。

将网桥组的相应号码分配给BVI时配置BVI。每个网桥组只能有一个对应的BVI。此示例将网桥组编号3分配给BVI。

router<configure>#interface BVI <2>

2. 为BVI分配IP地址。

router<config-if>#ip address 10.3.1.1 255.255.0.0

router<config-if>#no shut

为WPA-PSK身份验证配置SSID

完成以下操作：

1. 启用无线电接口。

要启用无线电接口，请转到DOT11无线电接口配置模式并为接口分配SSID。

router<config>#interface dot11radio0

router<config-if>#no shutdown

router<config-if>#ssid wpa-shared

2. 要启用WPA密钥管理，首先为VLAN接口配置WPA加密密码。本示例使用tkip作为加密密码。

键入此命令以指定无线电接口上的WPA密钥管理类型。

router<config>#interface dot11radio0

router(config-if)#encryption vlan 3 mode ciphers tkip

3. 将SSID绑定到VLAN。

   要在此接口上启用SSID，请在SSID配置模式下将SSID绑定到VLAN。

   router<config-ssid>vlan 3

4. 使用WPA-PSK身份验证配置SSID。

   您需要首先在SSID配置模式下配置开放或网络EAP身份验证，以启用WPA密钥管理。此示例配置开放式身份验证。

   router<config>#interface dot11radio0

   router<config-if>#ssid wpa-shared

   router<config-ssid>#authentication open

   现在，在SSID上启用WPA密钥管理。已为此VLAN配置密钥管理密码tkip。

   router(config-if-ssid)#authentication key-management wpa

   在SSID上配置WPA-PSK身份验证。

   router(config-if-ssid)#wpa-psk ascii 1234567890 !— 1234567890是此SSID的预共享密钥值。确保在客户端为此SSID指定相同的密钥。

5. 在无线电接口上启用VLAN。

   router<config>#interface Dot11Radio 0.3

   router<config-subif>#encapsulation dot1Q 3

   router<config-subif>#bridge-group 3

为此VLAN的无线客户端配置内部DHCP服务器

在全局配置模式下键入以下命令，配置此VLAN无线客户端的内部DHCP服务器：

- ip dhcp excluded-address 10.3.1.1 10.3.1.5
- ip dhcp pool wpa-psk

在DHCP池配置模式下，键入以下命令：

- network 10.3.0.0 255.255.0.0
- default-router 10.3.1.1

配置WPA（使用EAP）身份验证

这是另一个WPA密钥管理类型。在这里，客户端和身份验证服务器使用EAP身份验证方法相互进行身份验证，并且客户端和服务器生成成对主密钥(PMK)。使用WPA时，服务器会动态生成PMK并将其传递到接入点，但使用WPA-PSK时，您可在客户端和接入点上配置预共享密钥，该预共享密钥将用作PMK。

有关详细信息，请参阅采用EAP身份验证的WPA。

本示例使用以下配置设置：

- SSID名称：wpa-dot1x
- VLAN 4
- 内部DHCP服务器范围:10.4.0.0/16

在路由器上完成以下操作：

1. 配置集成路由和桥接(IRB)并设置网桥组
2. 配置桥接虚拟接口(BVI)
3. 为WPA身份验证配置本地RADIUS服务器。
4. 为采用EAP身份验证的WPA配置SSID
5. 为此VLAN的无线客户端配置内部DHCP服务器

配置集成路由和桥接(IRB)并设置网桥组

完成以下操作：

1. 在路由器中启用IRB。

   router<configure>#bridge irb

   注：如果所有安全类型都要在单个路由器上配置，则仅可在路由器上全局启用一次IRB就足够了。不需要为每个单独的身份验证类型启用它。

2. 定义网桥组。

   本示例使用网桥组编号4。

   router<configure>#bridge 4

3. 选择网桥组的生成树协议。

   此处，为此网桥组配置了IEEE生成树协议。

router<configure>#bridge 4 protocol ieee

4. 启用BVI以接受和路由从对应网桥组接收的可路由数据包。

   此示例使BVI能够接受和路由IP数据包。

   router<configure>#bridge 4 route ip

配置桥接虚拟接口(BVI)

完成以下操作：

1. 配置BVI。

   将网桥组的相应号码分配给BVI时配置BVI。每个网桥组只能有一个对应的BVI。此示例将网桥组编号4分配给BVI。

   router<configure>#interface BVI <4>

2. 为BVI分配IP地址。

   router<config-if>#ip address 10.4.1.1 255.255.0.0

   router<config-if>#no shut

为WPA身份验证配置本地RADIUS服务器

有关详细信息，请参阅802.1x/EAP身份验证一节。

为采用EAP身份验证的WPA配置SSID

完成以下操作：

1. 启用无线电接口。

   要启用无线电接口，请转到DOT11无线电接口配置模式并为接口分配SSID。

   router<config>#interface dot11radio0

   router<config-if>#no shutdown

   router<config-if>#ssid wpa-dot1x

2. 要启用WPA密钥管理，首先为VLAN接口配置WPA加密密码。本示例使用tkip作为加密密码。

   键入此命令以指定无线电接口上的WPA密钥管理类型。

   router<config>#interface dot11radio0

   router(config-if)#encryption vlan 4 mode ciphers tkip

3. 将SSID绑定到VLAN。

   要在此接口上启用SSID，请在SSID配置模式下将SSID绑定到VLAN。

   vlan 4

4. 使用WPA-PSK身份验证配置SSID。

   要为WPA配置具有EAP身份验证的无线接口，首先为网络EAP配置关联的SSID。

   router<config>#interface dot11radio0

   router<config-if>#ssid wpa-shared

   router<config-ssid>#authentication network eap eap_methods

5. 现在，在SSID上启用WPA密钥管理。已为此VLAN配置密钥管理密码tkip。

   router(config-if-ssid)#authentication key-management wpa

6. 在无线电接口上启用VLAN。

   router<config>#interface Dot11Radio 0.4

   router<config-subif>#encapsulation dot1Q 4

   router<config-subif>#bridge-group 4

为此VLAN的无线客户端配置内部DHCP服务器

在全局配置模式下键入以下命令，配置此VLAN无线客户端的内部DHCP服务器：

- ip dhcp excluded-address 10.4.1.1 10.4.1.5
- ip dhcp pool wpa-dot1shared

在DHCP池配置模式下，键入以下命令：

- network 10.4.0.0 255.255.0.0
- default-router 10.4.1.1

配置无线客户端进行身份验证

配置ISR后，按照说明为无线客户端配置不同的身份验证类型，以便路由器可以对这些无线客户端进行身份验证并提供对WLAN网络的访问。本文档使用Cisco Aironet Desktop Utility(ADU)进行客户端配置。

配置无线客户端进行开放式身份验证

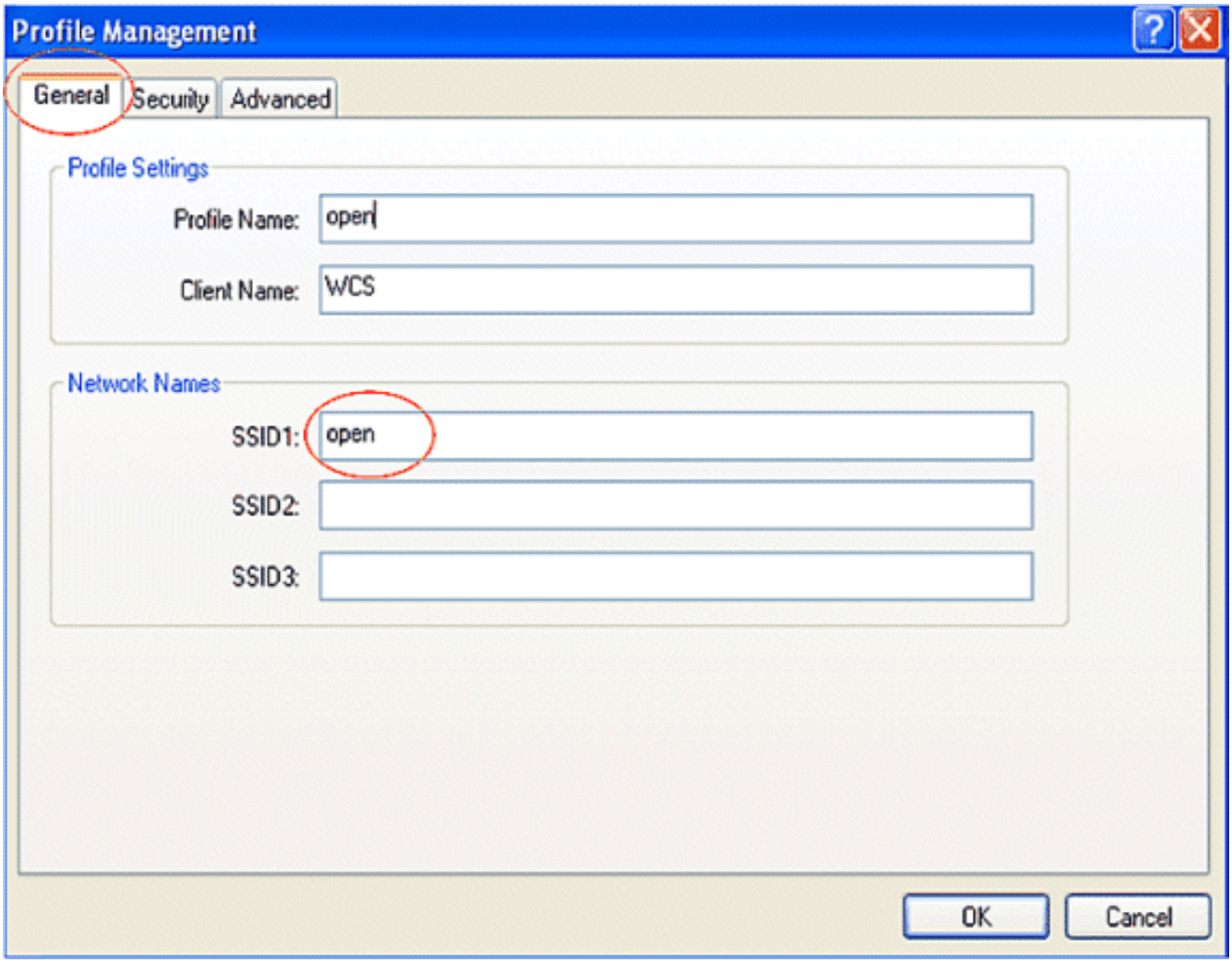
请完成以下步骤：

1. 在 ADU 上的“Profile Management”窗口中，单击 New 以创建一个新配置文件。

   系统将显示一个新窗口，您可以在其中设置开放式身份验证的配置。在General选项卡下，输入客户端适配器使用的配置文件名称和SSID。

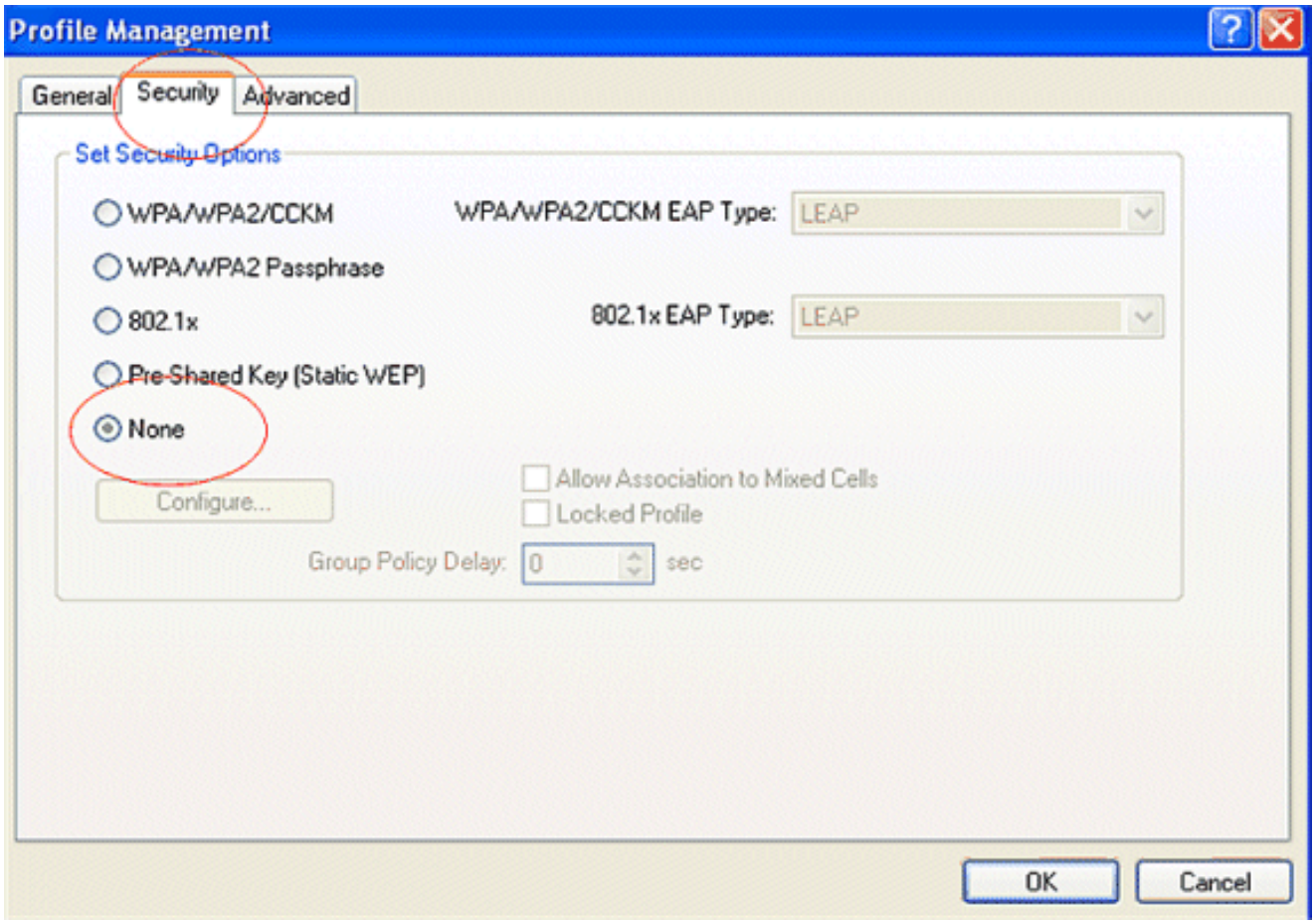
   在本示例中，配置文件名称和SSID为open。

   注意：SSID必须与您在ISR上为开放式身份验证配置的SSID匹配。

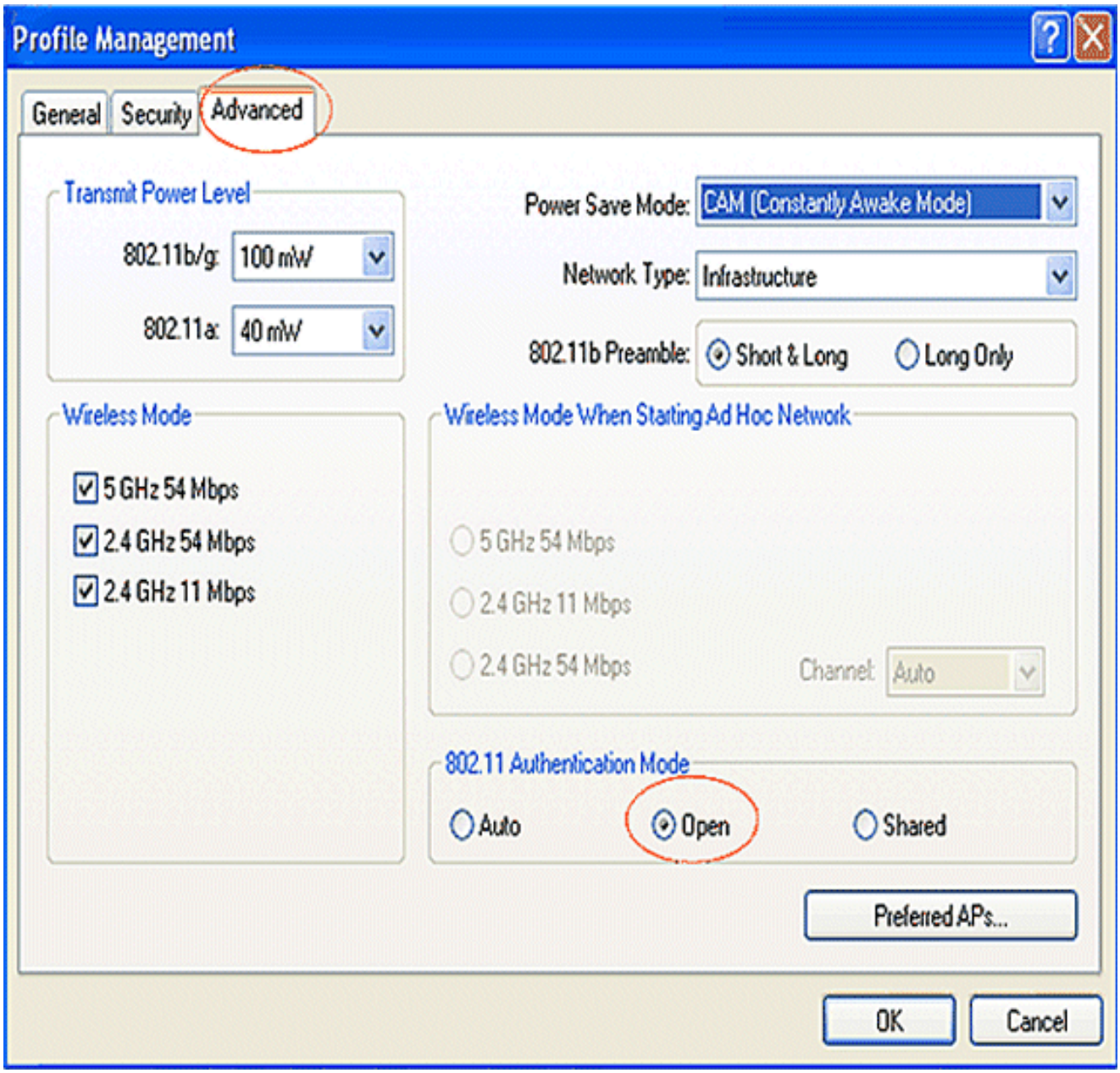


2. 单击Security选项卡，并将WEP加密的安全选项保留为None。由于本示例使用WEP作为可选操作，因此将此选项设置为None将允许客户端成功关联并与WLAN网络通信。

   单击 OK

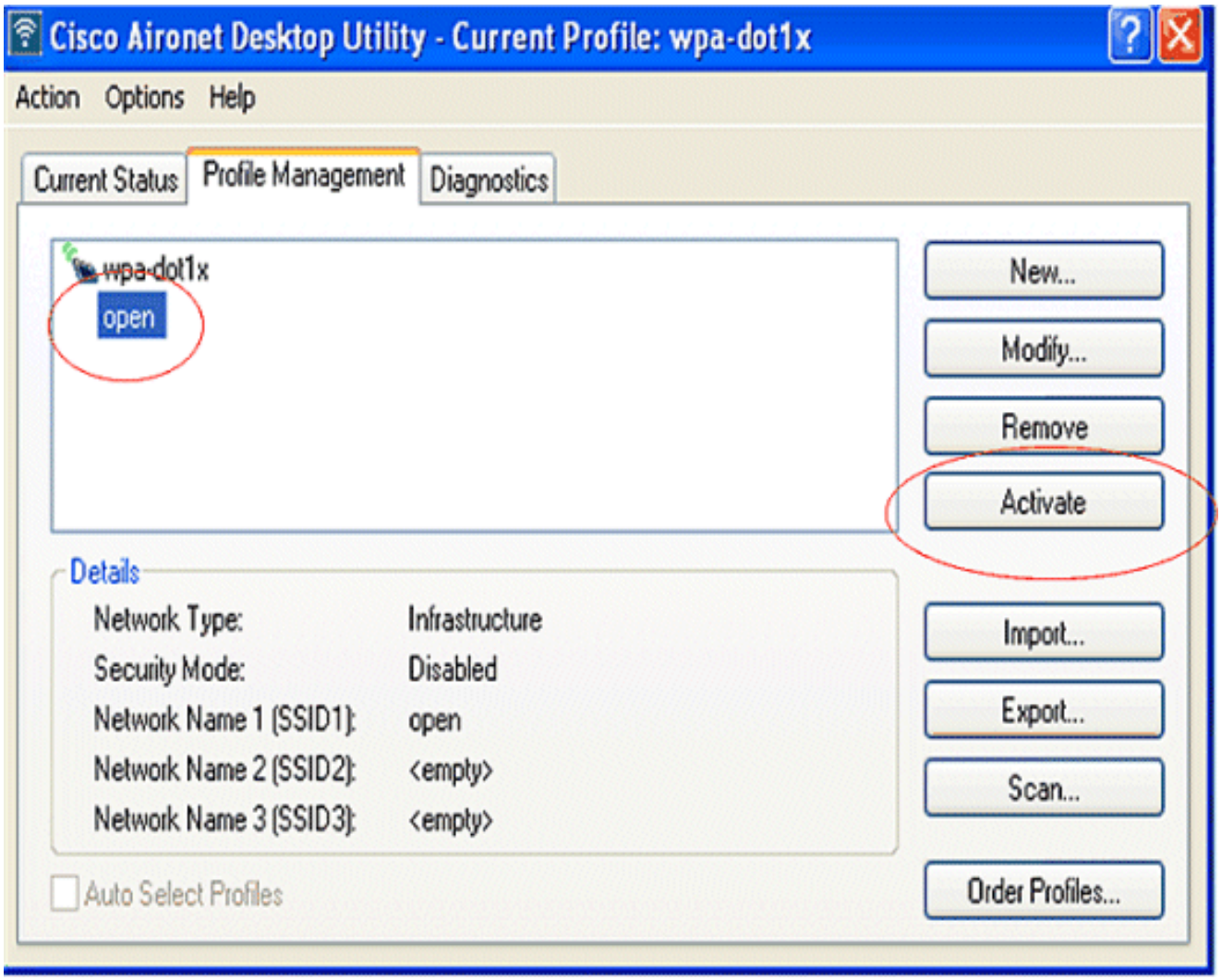


3. 从Profile Management选项卡中选择Advanced窗口，并将802.11 Authentication Mode设置为Open，以进行开放式身份验证。

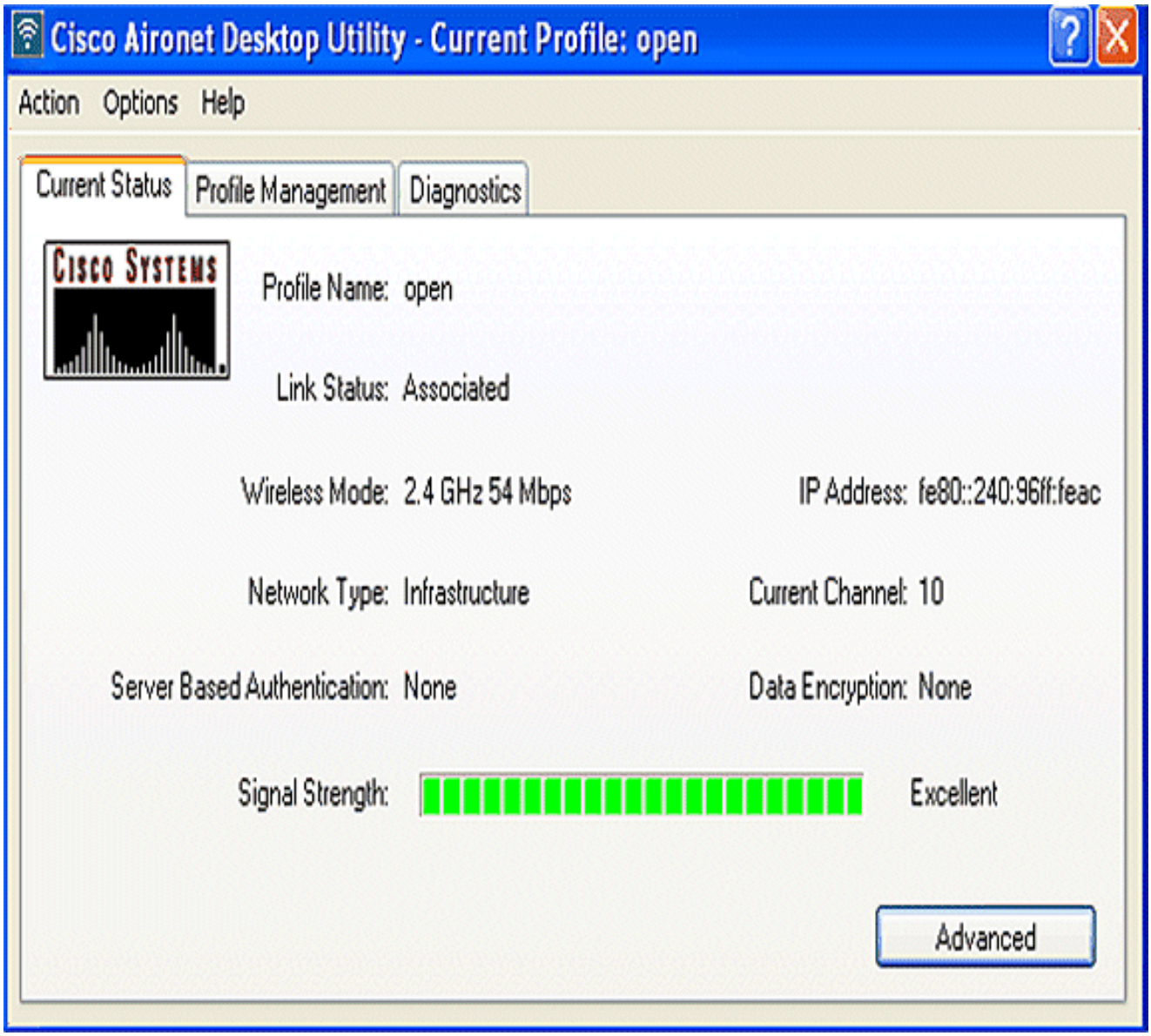


使用本部分可确认配置能否正常运行。

1. 创建客户端配置文件后，点击Profile Management选项卡下的Activate激活配置文件。



2. 检查ADU状态以成功进行身份验证。



配置无线客户端进行802.1x/EAP身份验证

请完成以下步骤：

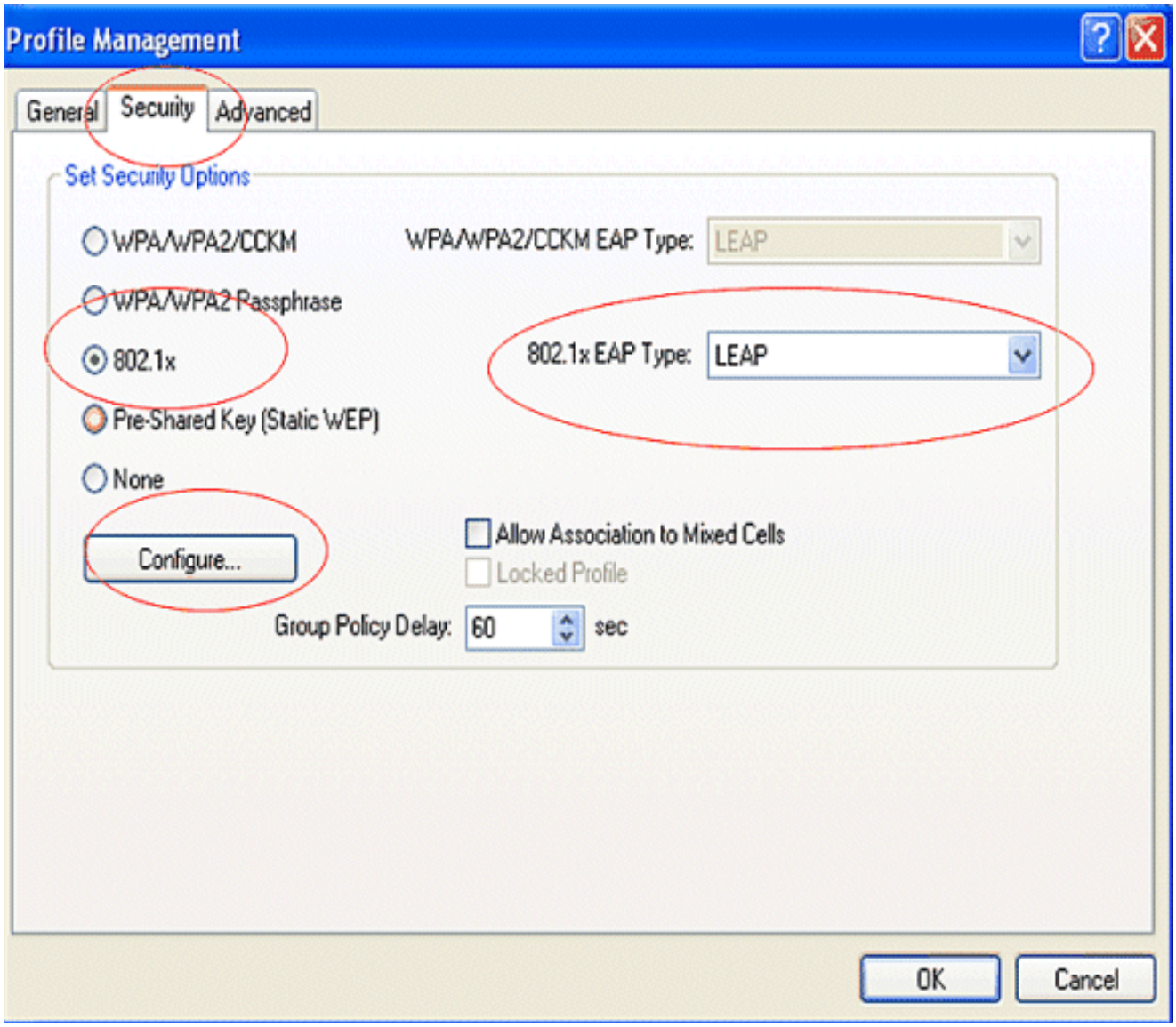
1. 在 ADU 上的“Profile Management”窗口中，单击 New 以创建一个新配置文件。

   系统将显示一个新窗口，您可以在其中设置开放式身份验证的配置。在General选项卡下，输入客户端适配器使用的配置文件名称和SSID。

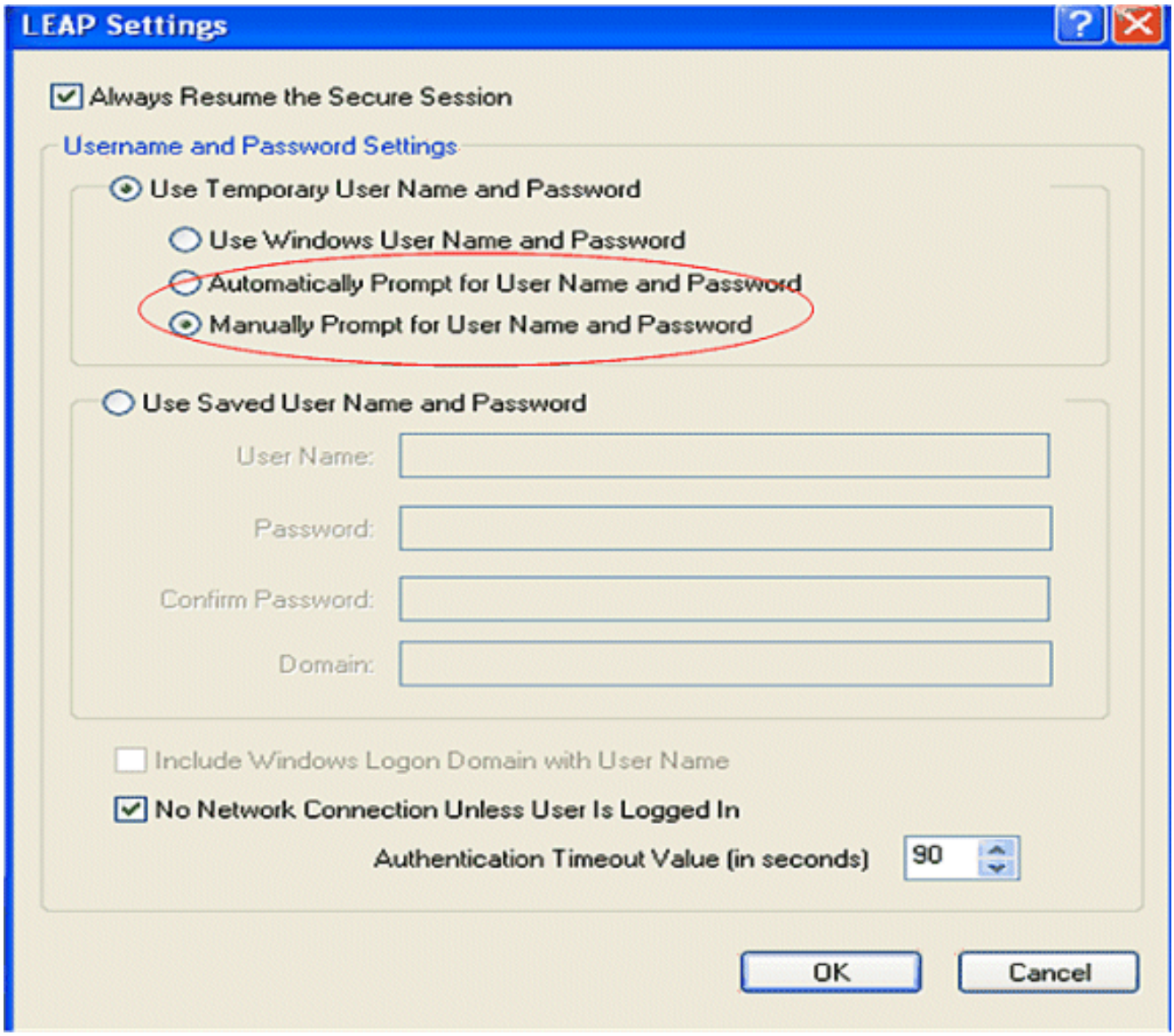
   在本示例中，配置文件名称和SSID是leap。

2. 在Profile Management下，单击Security选项卡，将安全选项设置为802.1x，然后选择适当的EAP类型。本文档使用LEAP作为身份验证的EAP类型。现在，单击Configure以配置LEAP用户名和密码设置。

   注意：注意：SSID必须与您在ISR上为802.1x/EAP身份验证配置的SSID匹配。

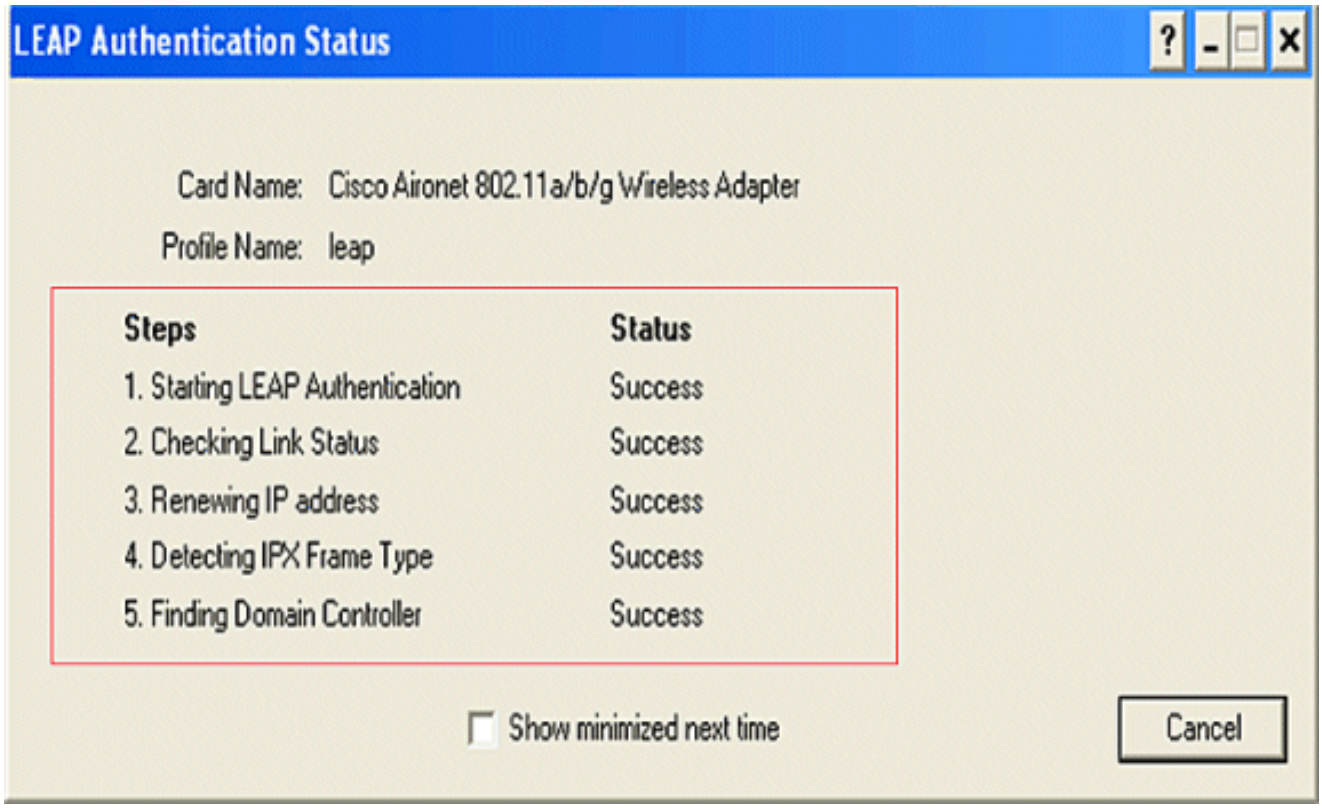


3. 在用户名和密码设置下，此示例选择Manually Prompt for User Name and Password，以便在客户端尝试连接到网络时提示客户端输入正确的用户名和密码。Click OK.



使用本部分可确认配置能否正常运行。

- 创建客户端配置文件后，点击Profile Management选项卡下的Activate以激活配置文件跳跃。系统将提示您输入leap用户名和密码。本示例使用用户名和密码user1。Click OK.
- 您可以监视客户端身份验证成功，并从路由器上配置的DHCP服务器分配IP地址。



配置无线客户端进行WPA-PSK身份验证

请完成以下步骤：

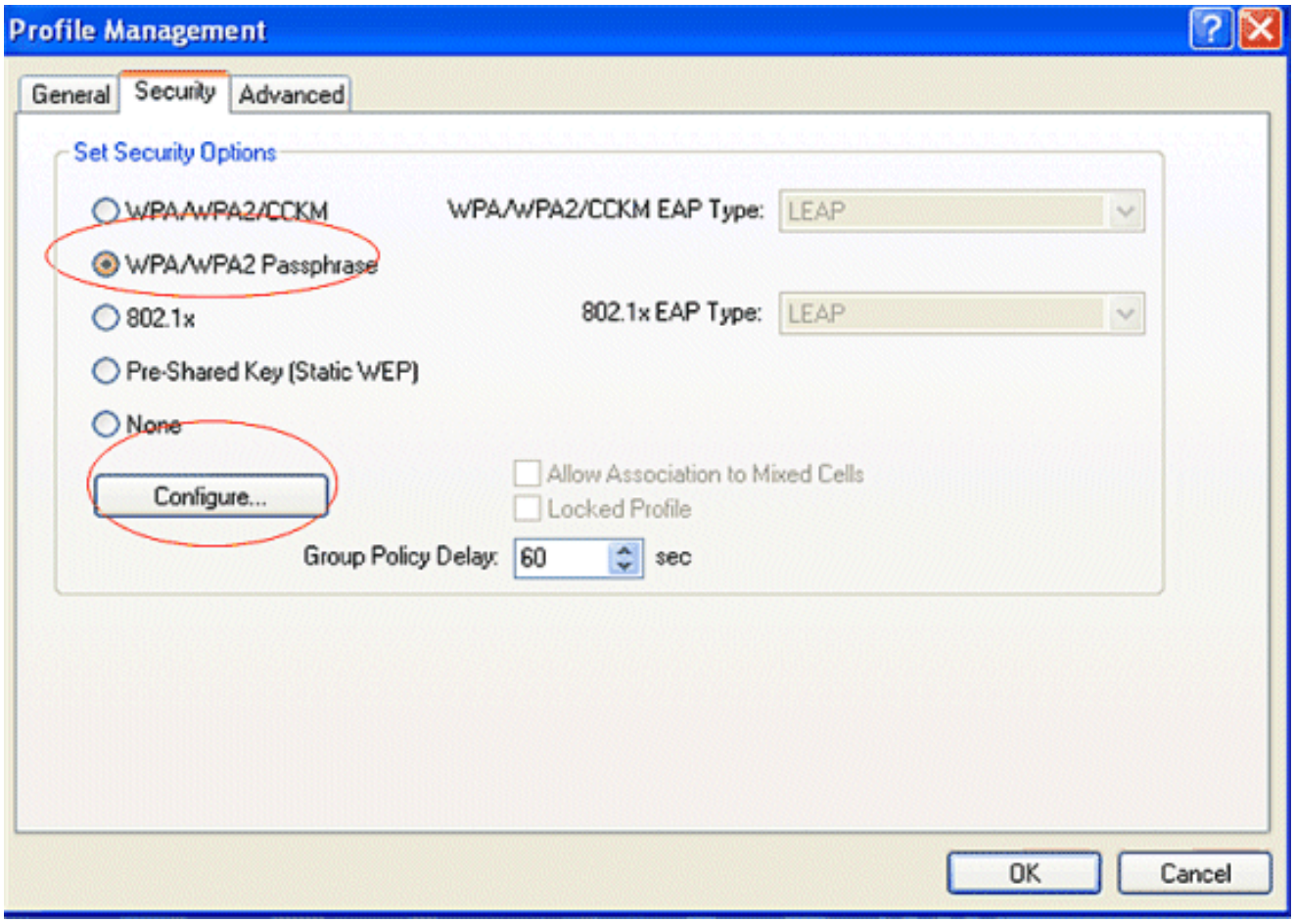
1. 在 ADU 上的“Profile Management”窗口中，单击 New 以创建一个新配置文件。

   系统将显示一个新窗口，您可以在其中设置开放式身份验证的配置。在General选项卡下，输入客户端适配器使用的Profile Name和SSID。

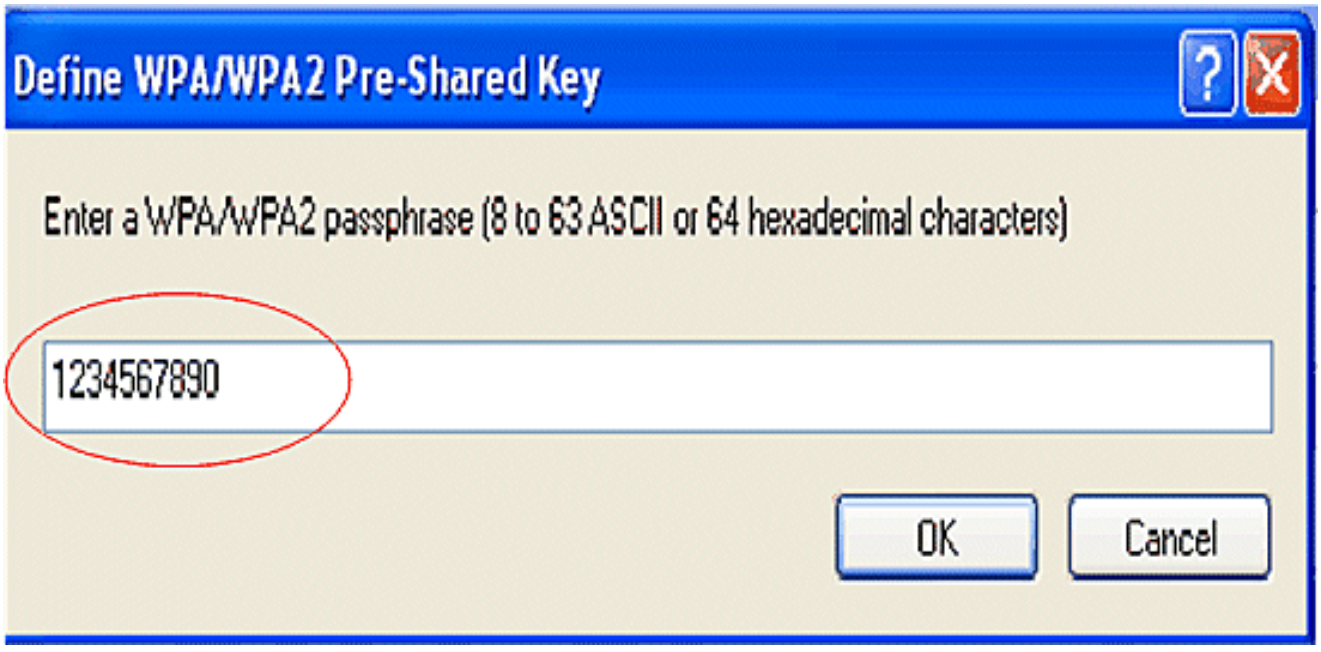
   在本示例中，配置文件名称和SSID是wpa-shared。

   注意：SSID必须与您在ISR上为WPA-PSK身份验证配置的SSID匹配。

2. 在Profile Management下，单击Security选项卡，并将安全选项设置为WPA/WPA2 Passphrase。现在，单击Configure以配置WPA口令。

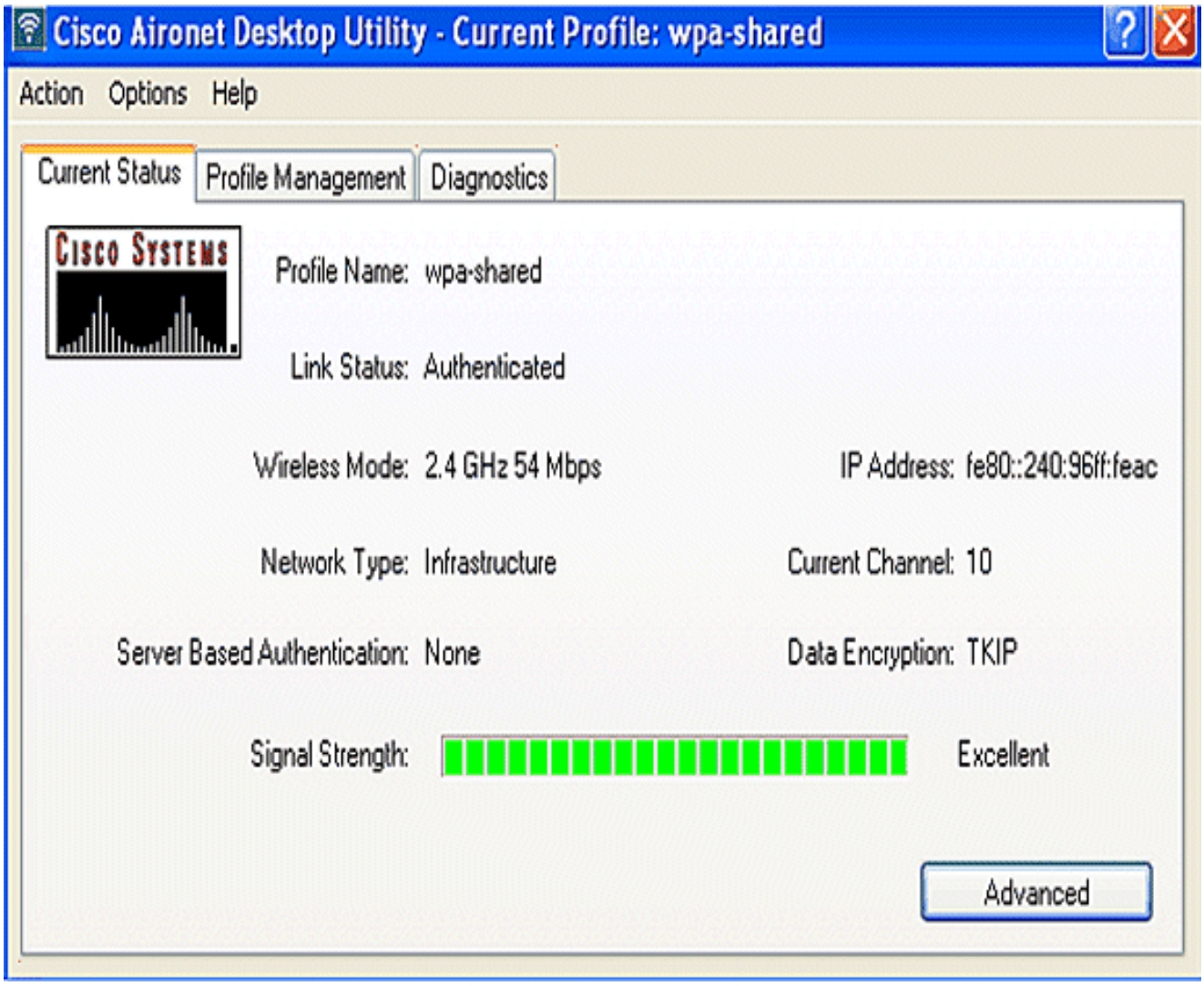


3. 定义WPA预共享密钥。密钥的长度必须为8到63个ASCII字符。Click OK.



使用本部分可确认配置能否正常运行。

- 创建客户端配置文件后，单击Profile Management选项卡下的Activate以激活配置文件wpa-shared。
- 检查ADU是否成功进行身份验证。



为WPA（采用EAP）身份验证配置无线客户端

请完成以下步骤：

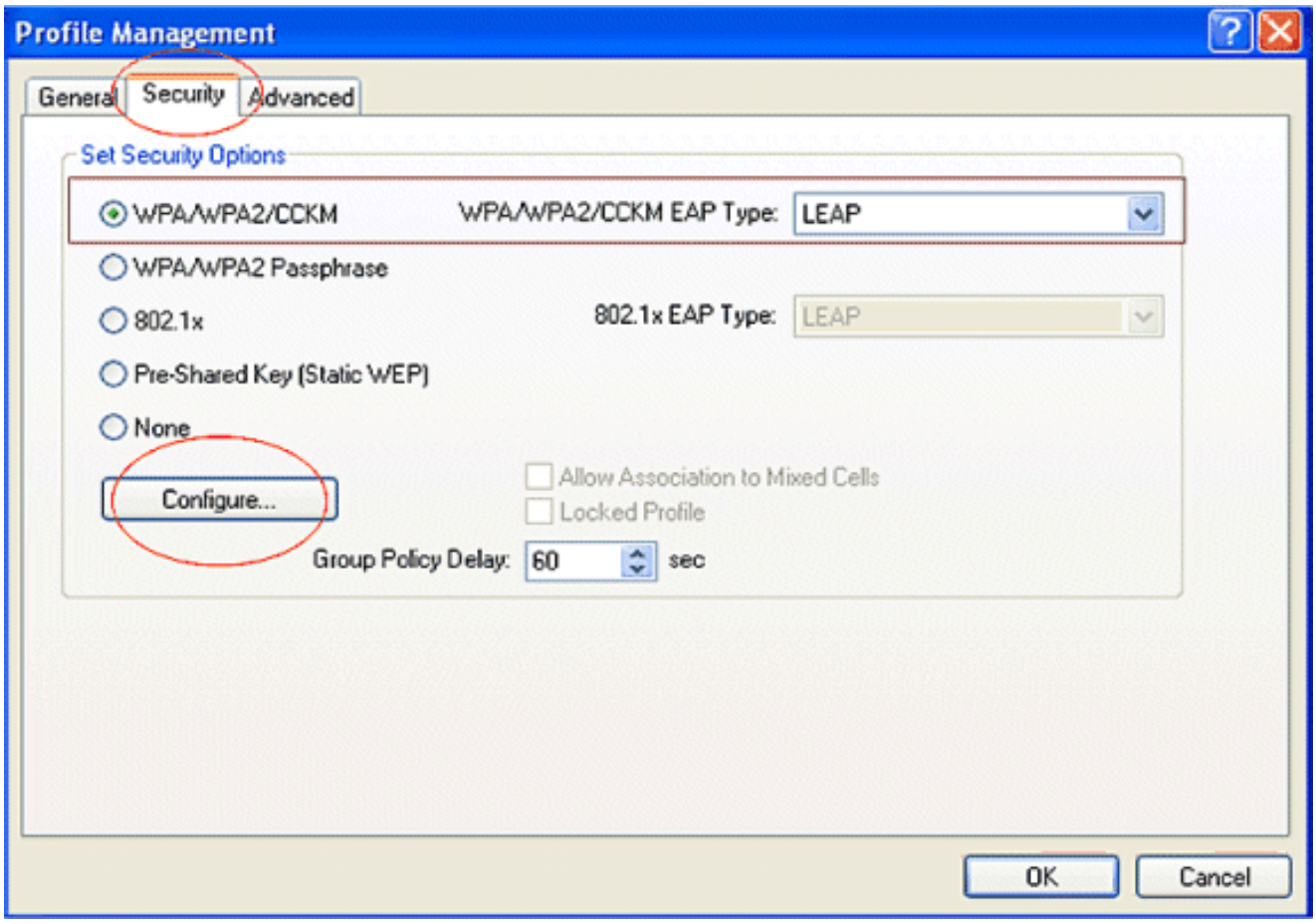
1. 在 ADU 上的“Profile Management”窗口中，单击 New 以创建一个新配置文件。

   系统将显示一个新窗口，您可以在其中设置开放式身份验证的配置。在General选项卡下，输入客户端适配器使用的配置文件名称和SSID。

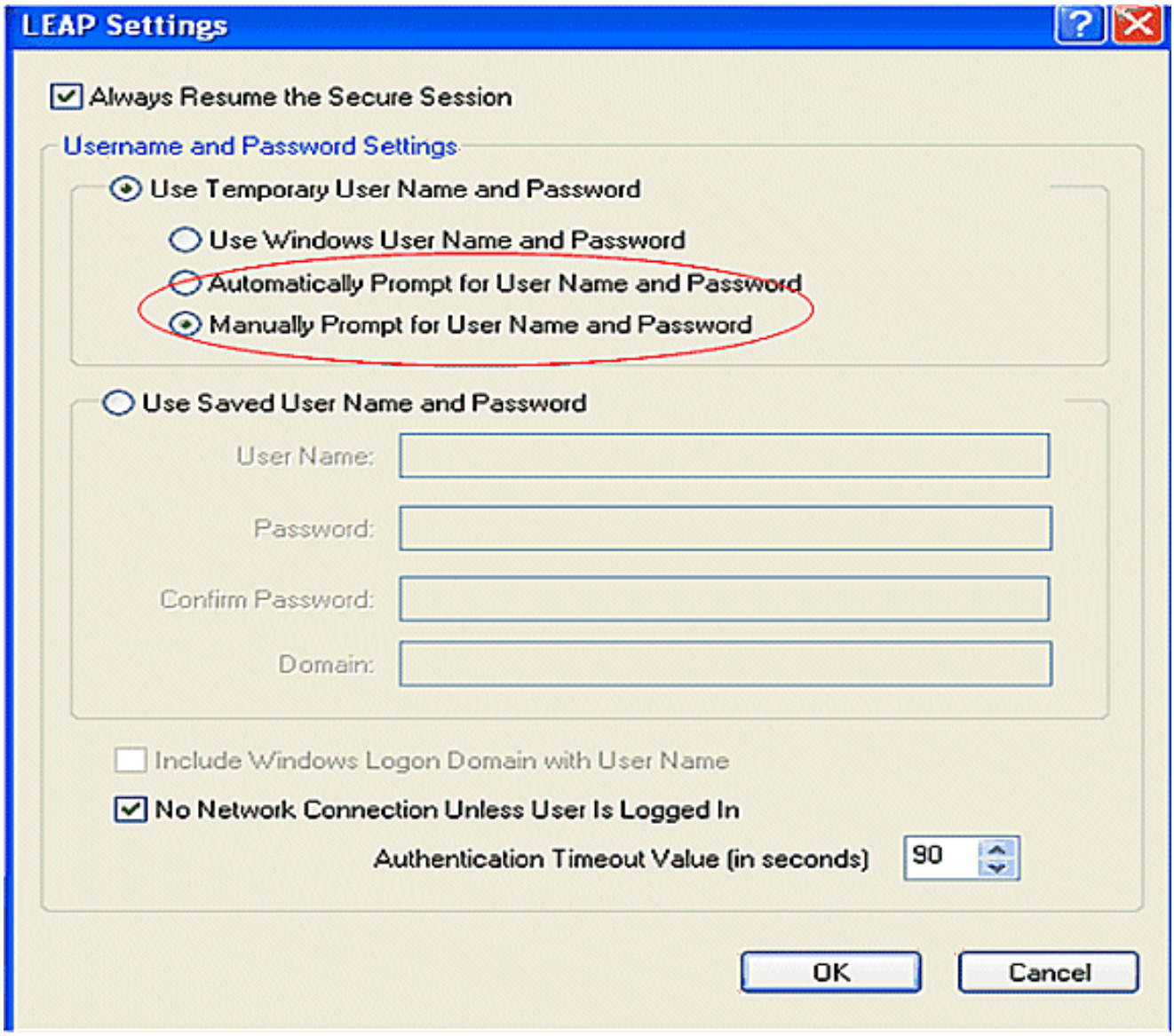
   在本示例中，配置文件名称和SSID是wpa-dot1x。

   注意：SSID必须与您在ISR上为WPA（使用EAP）身份验证配置的SSID匹配。

2. 在Profile Management下，单击Security选项卡，将安全选项设置为WPA/WPA2/CCKM，然后选择适当的WPA/WPA2/CCKM EAP类型。本文档使用LEAP作为身份验证的EAP类型。现在，单击Configure以配置LEAP用户名和密码设置。

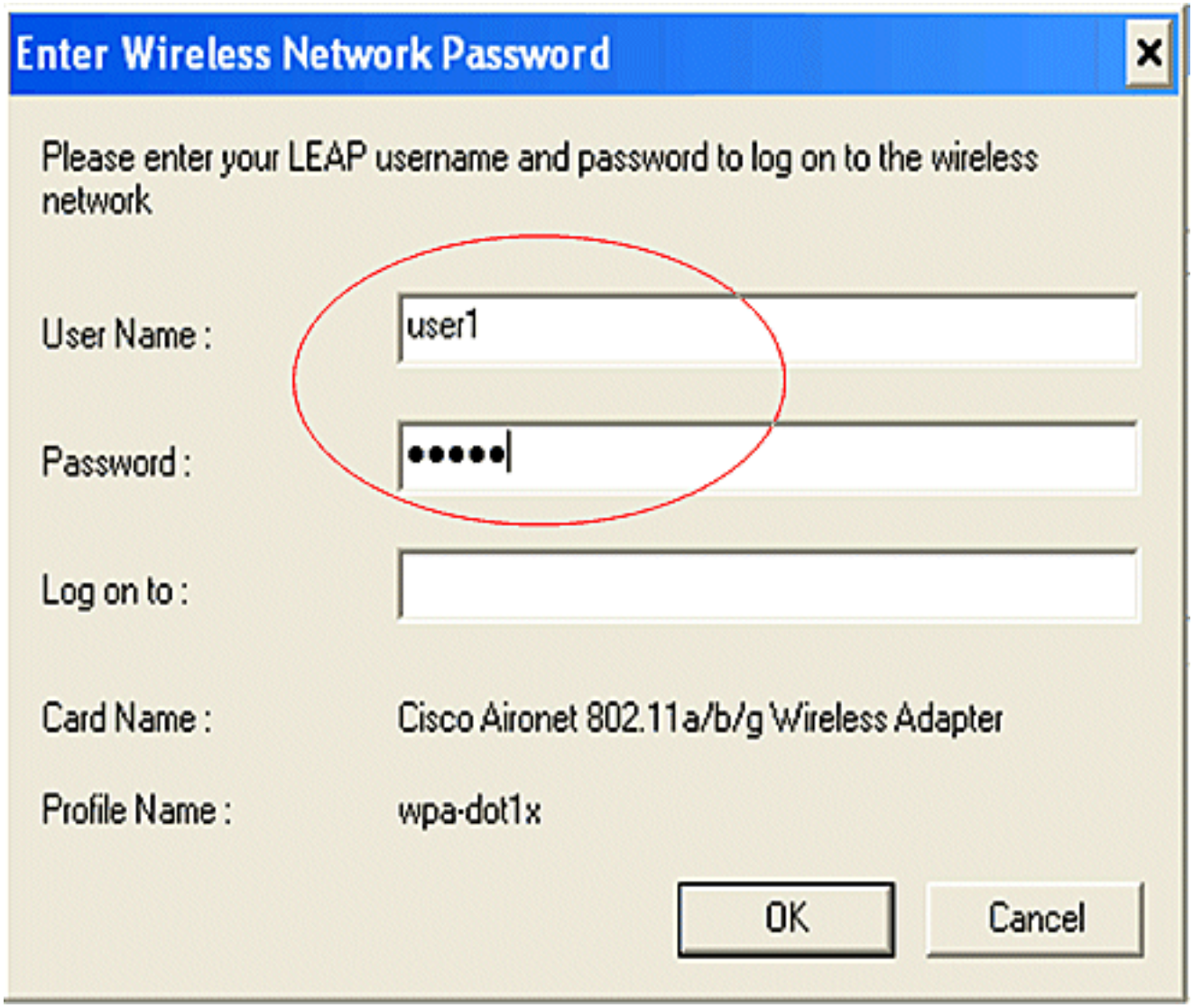


3. 在Username and Password Settings区域下，此示例选择Manually Prompt for User Name and Password，以便在客户端尝试连接到网络时提示客户端输入正确的用户名和密码。Click OK.

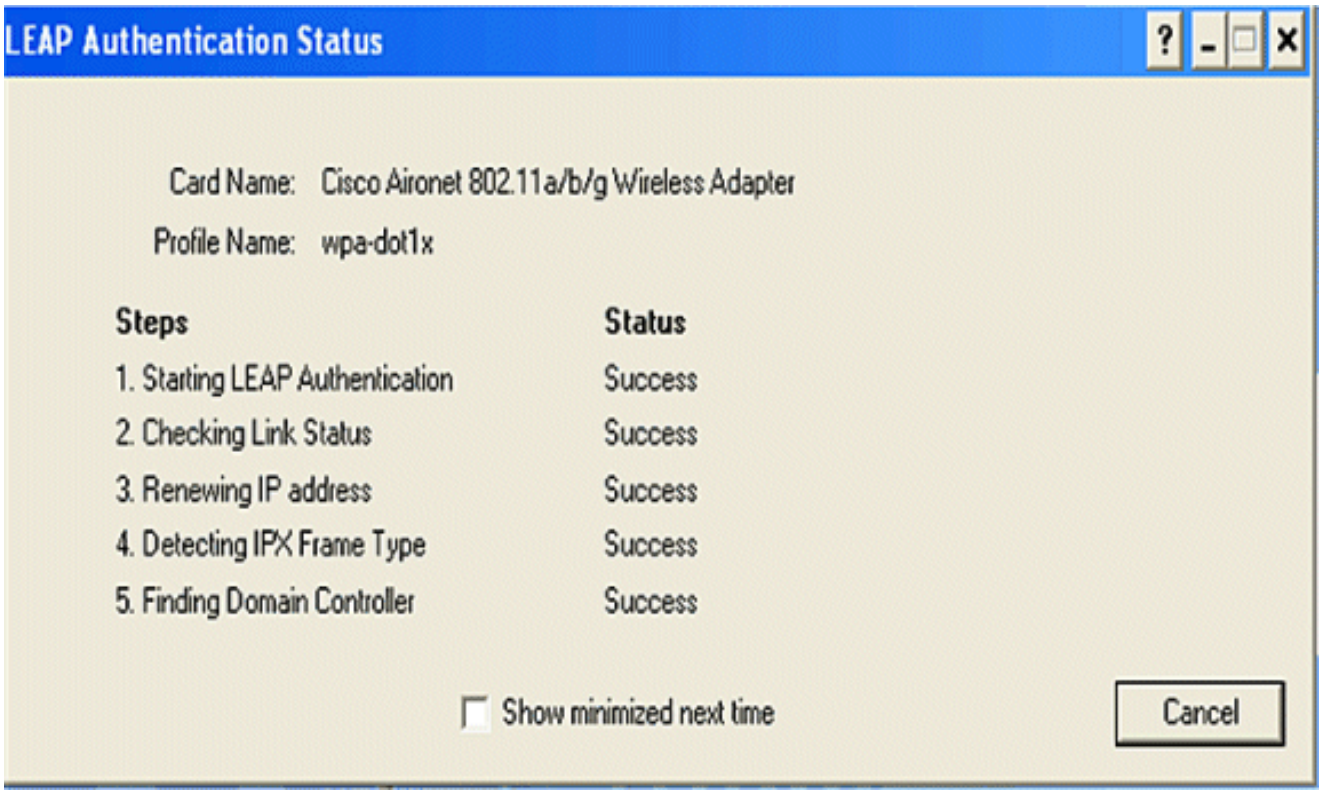


使用本部分可确认配置能否正常运行。

1. 创建客户端配置文件后，点击Profile Management选项卡下的Activate以激活配置文件wpa-dot1x。系统将提示您输入LEAP用户名和密码。本示例将用户名和密码用作user1。Click OK.



2. 您可以监视客户端成功进行身份验证。



来自路由器CLI的show dot11 associations命令可显示有关客户端关联状态的完整详细信息。下面是一个示例。

Router#show dot11 associations

<#root>

```
802.11 Client Stations on Dot11Radio0:

SSID [leap] :

MAC Address    IP address      Device        Name            Parent         State
0040.96ac.e657 10.3.0.2        CB21AG/PI21AG WCS             self        EAP-Assoc


SSID [open] :

SSID [pre-shared] : DISABLED, not associated with a configured VLAN

SSID [wpa-dot1x] :

SSID [wpa-shared] :


Others:  (not related to any ssid)
```

故障排除

故障排除命令

可使用以下 debug 命令对配置进行故障排除。

- debug dot11 aaa authenticator all — 激活MAC和EAP身份验证数据包的调试。
- debug radius authentication — 显示服务器和客户端之间的RADIUS协商。
- debug radius local-server packets — 显示发送和接收的RADIUS数据包的内容。
- debug radius local-server client — 显示有关客户端身份验证失败的错误消息。

相关信息

- 无线局域网控制器认证的配置示例
- 在接入点上配置VLAN
- 带内部DHCP和开放式认证的1800 ISR无线路由器配置示例
- 思科无线ISR和HWIC接入点配置指南
- 使用带 WEP 加密和 LEAP 认证的 ISR 连接无线局域网配置示例
- 技术支持和文档 - Cisco Systems
- 配置身份验证类型
- 使用带 WEP 加密和 LEAP 认证的 ISR 连接无线局域网配置示例

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）。