使用ACS 5.2和WLC配置PEAP和EAP-FAST

目录

简介

本文档说明如何使用外部RADIUS服务器(例如访问控制服务器(ACS)5.2)配置无线LAN控制器(WLC)以进行可扩展身份验证协议(EAP)身份验证。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 具有WLC和轻量接入点(LAP)的基本知识
- 具有AAA服务器的功能知识
- 全面了解无线网络和无线安全问题

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件版本 7.0.220.0 的 Cisco 5508 WLC
- Cisco 3502 系列 LAP
- 带英特尔6300-N驱动程序14.3版的Microsoft Windows 7本地请求方
- 运行 5.2 版的 Cisco 安全 ACS
- Cisco 3560 系列交换机

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。

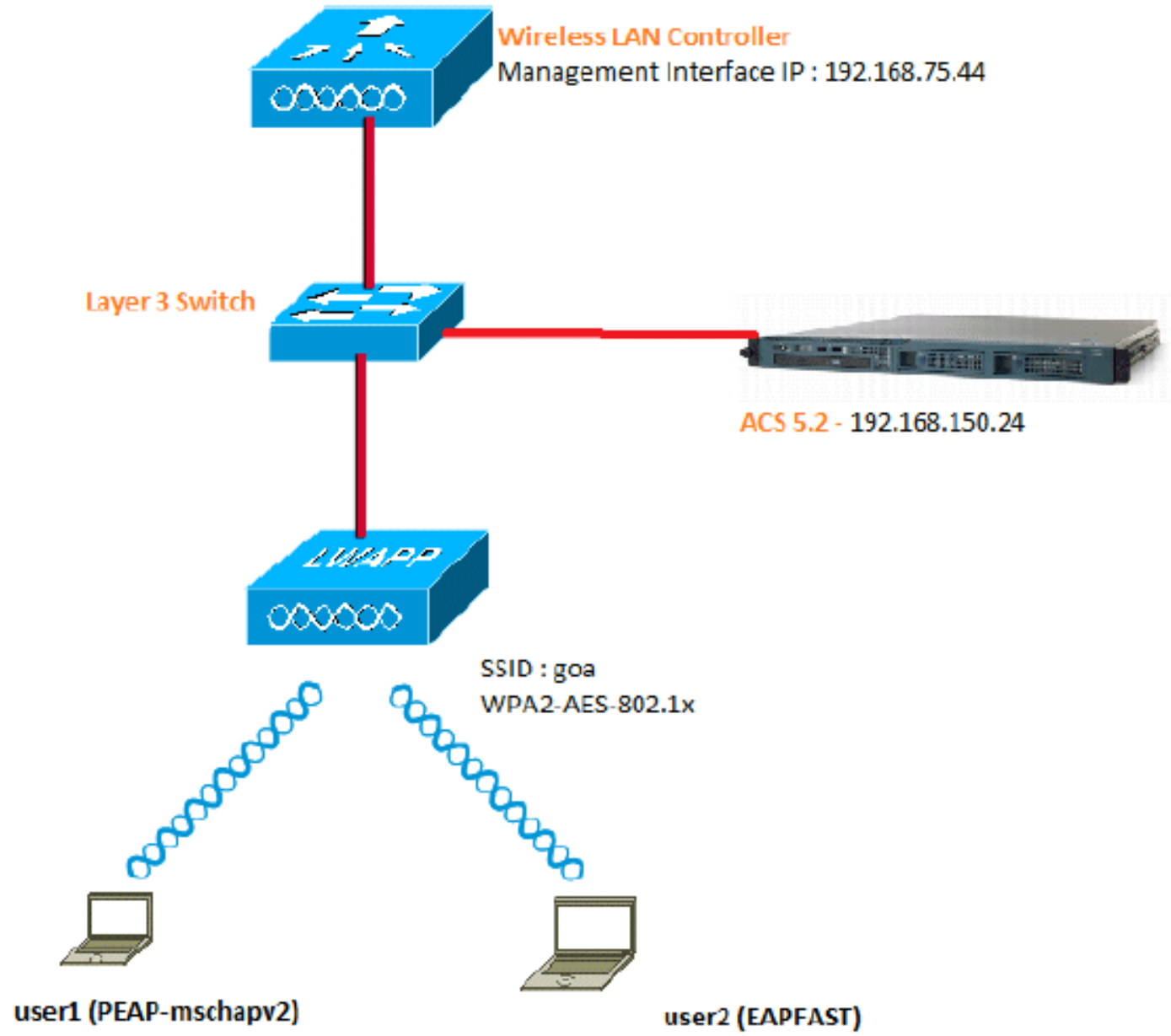
配置

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：



下面是此图中使用的组件的配置详细信息：

- ACS (RADIUS) 服务器的 IP 地址为 192.168.150.24。
- WLC的管理和AP管理器接口地址为192.168.75.44。
- DHCP服务器地址为192.168.150.25。
- 整个配置中都使用VLAN 253。两个用户都连接到同一个SSID“goa”。但是，user1配置为使用PEAP-MSCHAPv2进行身份验证，user2配置为使用EAP-FAST进行身份验证。
- 用户将分配到VLAN 253中：
  - VLAN 253:192.168.153.x/24。网关：192.168.153.1
  - VLAN 75:192.168.75.x/24。网关：192.168.75.1

假设

- 所有第3层VLAN都配置了交换机。
- 为DHCP服务器分配了一个DHCP作用域。
- 网络中的所有设备之间都存在第3层连接。
- LAP已连接到WLC。
- 每个VLAN都使用/24掩码。
- ACS 5.2已安装自签名证书。

配置步骤

此配置分为三个高级步骤：

1. 配置 RADIUS 服务器。
2. 配置WLC。
3. 配置无线客户端实用程序。

配置 RADIUS 服务器

RADIUS服务器配置分为四个步骤：

1. 配置网络资源。
2. 配置用户.
3. 定义策略元素。
4. 应用访问策略。

ACS 5.x是基于策略的访问控制系统。也就是说，ACS 5.x使用基于规则的策略模型，而不是4.x版本中使用的基于组的模型。

ACS 5.x基于规则的策略模型提供比旧的基于组的方法更强大、更灵活的访问控制。

在旧的基于组的模型中，一个组定义策略，因为它包含三种类型的信息并将它们关联在一起：

- 身份信息 — 此信息可以基于AD或LDAP组中的成员资格或内部ACS用户的静态分配。
- 其他限制或条件 — 时间限制、设备限制等。
- 权限 — VLAN或Cisco IOS®权限级别。

ACS 5.x策略模型基于以下形式的规则：

- 如果condition，则结果

例如，我们使用为基于组的模型描述的信息：

- 如果为identity-condition、restriction-condition，则为authorization-profile。

因此，我们可以灵活地限制在什么条件下允许用户访问网络，以及在满足特定条件时允许什么授权级别。

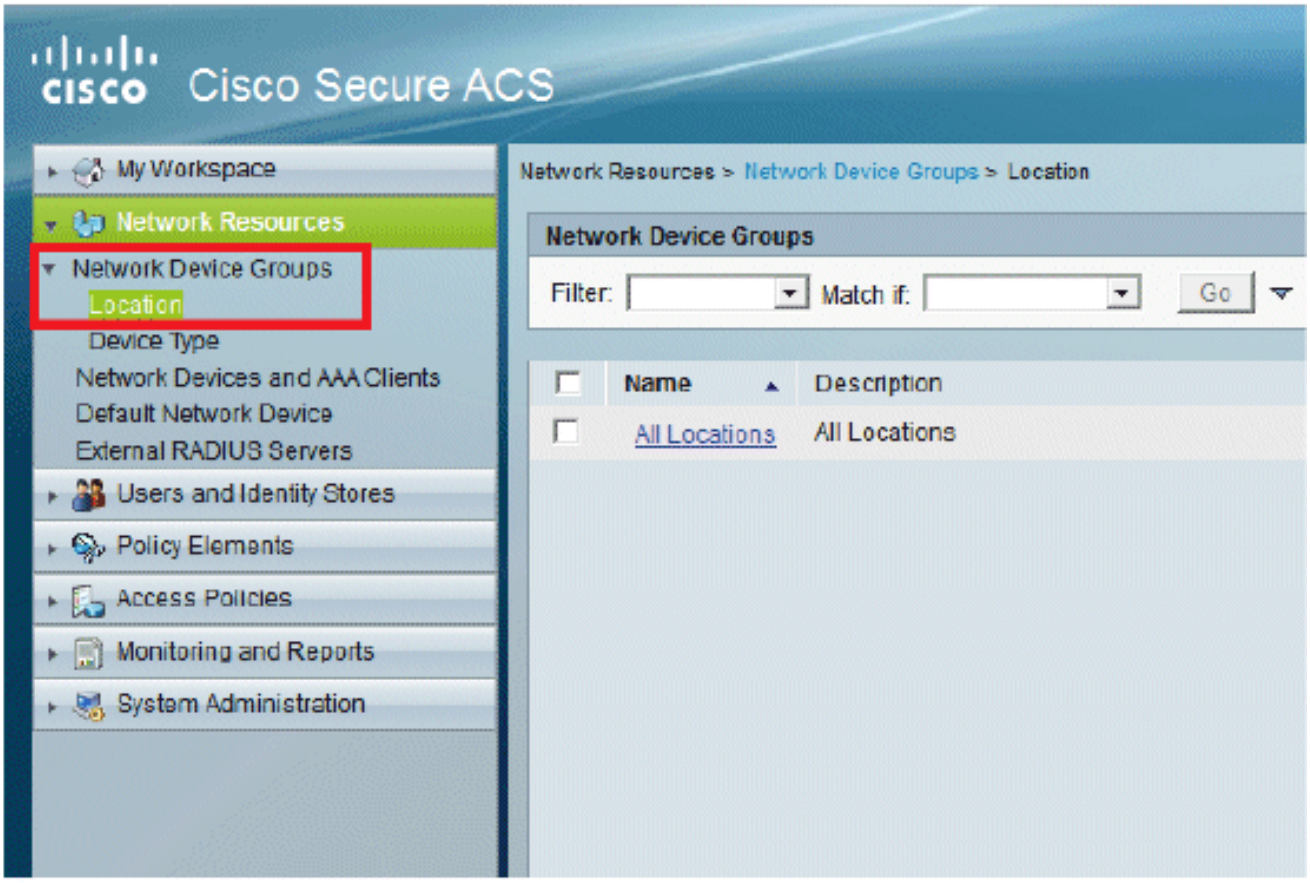
配置网络资源

在本节中，我们将为RADIUS服务器上的WLC配置AAA客户端。

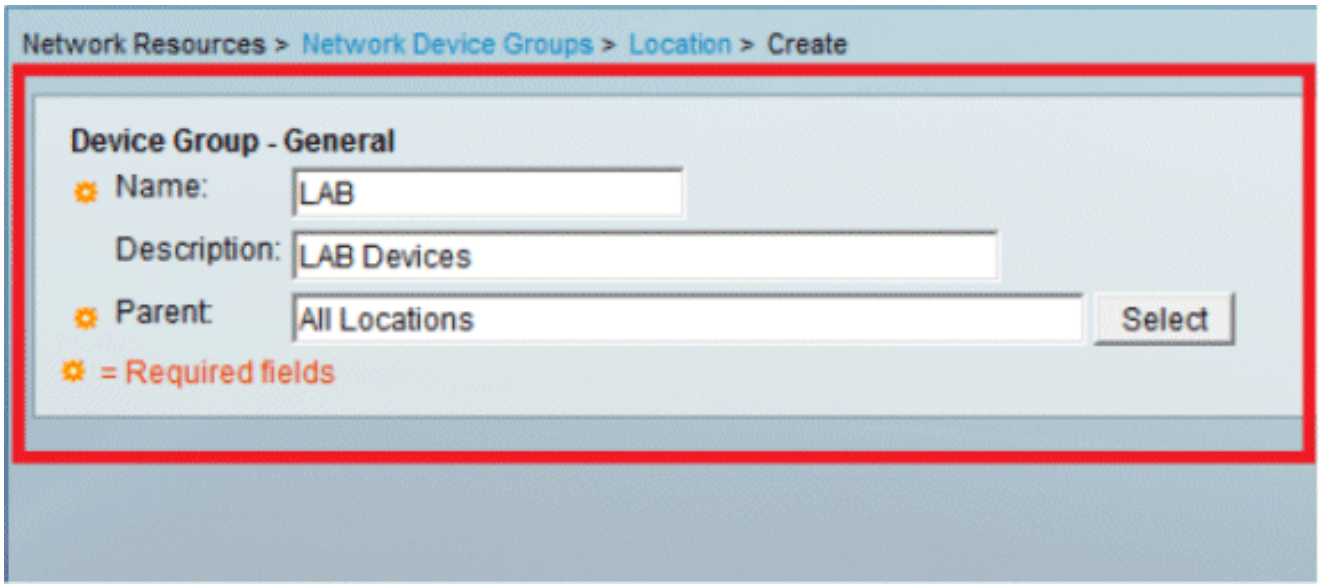
此过程说明如何在 RADIUS 服务器上将 WLC 添加为 AAA 客户端，以便 WLC 可以将用户凭证传递到 RADIUS 服务器。

请完成以下步骤：

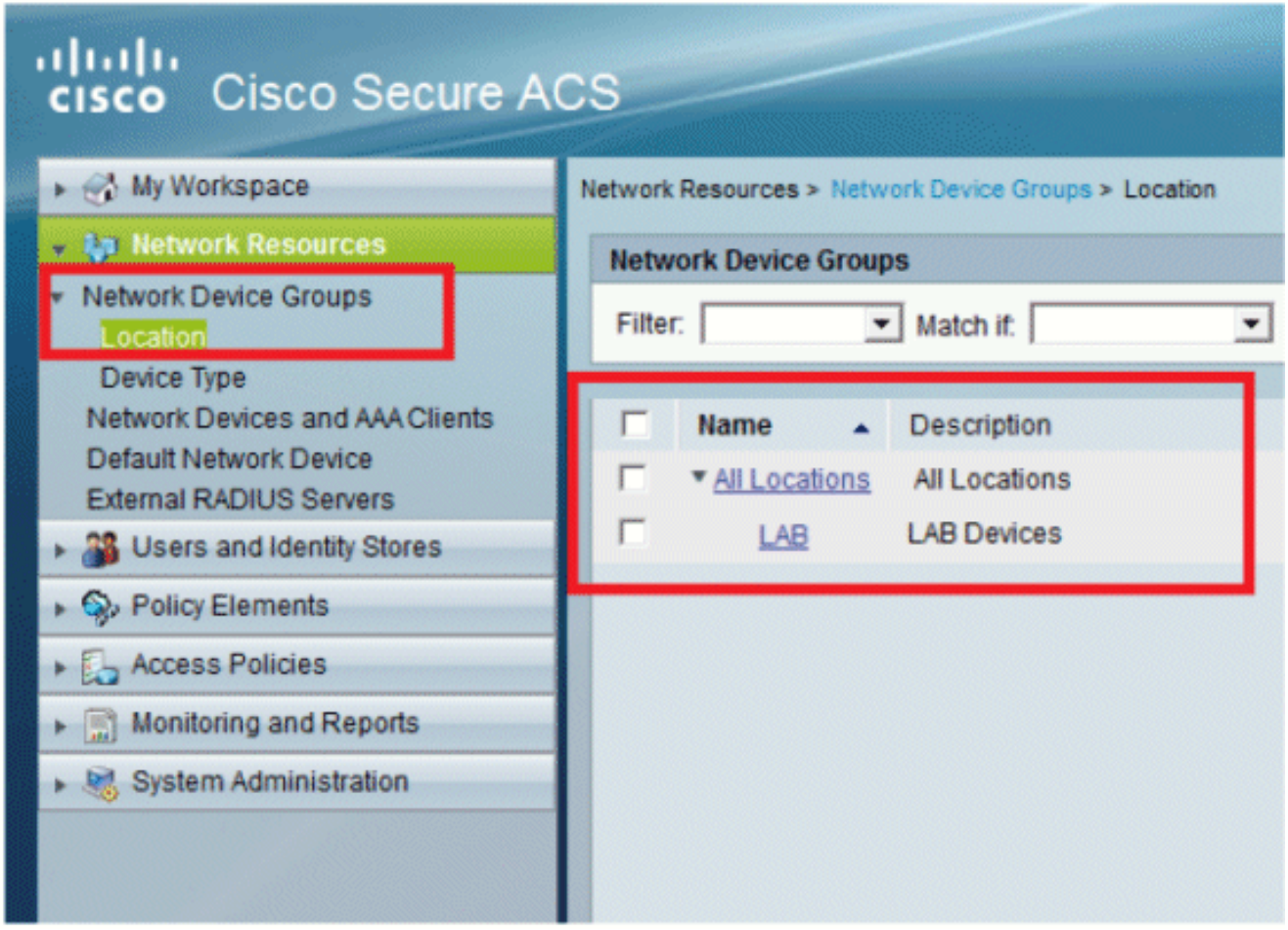
1. 从ACS GUI中，转到Network Resources > Network Device Groups > Location，然后单击Create（位于底部）。



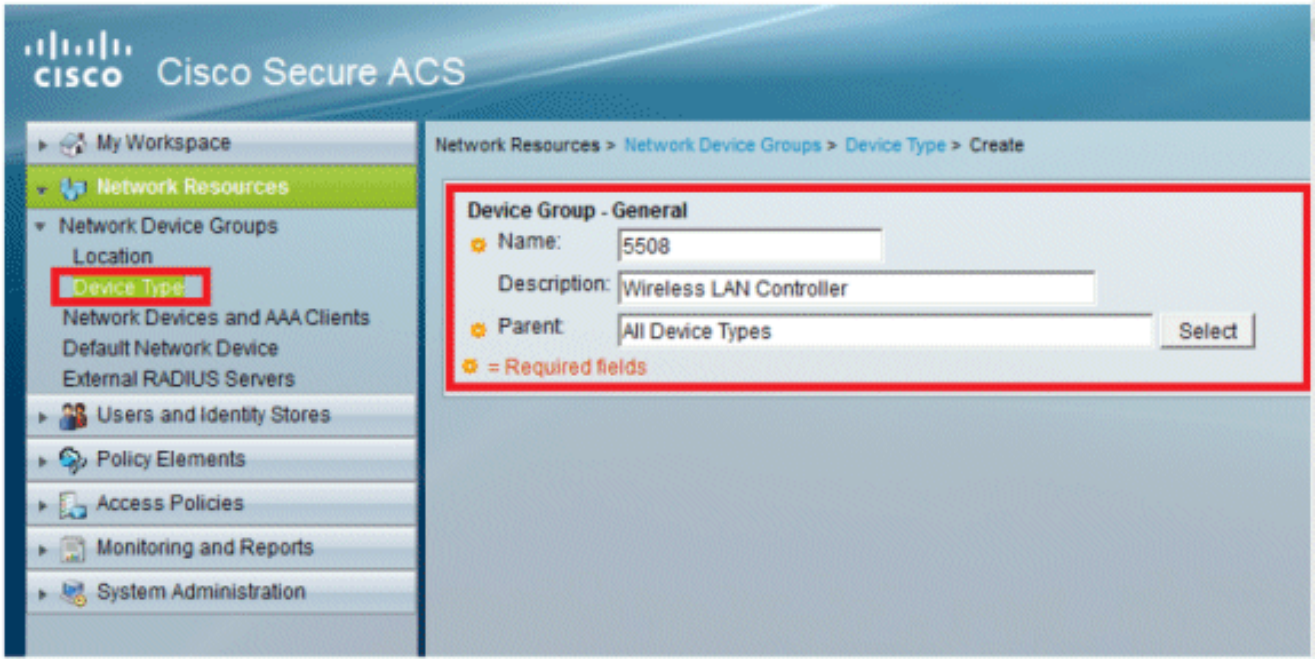
2. 添加必填字段，然后单击Submit。



现在您将看到以下屏幕：



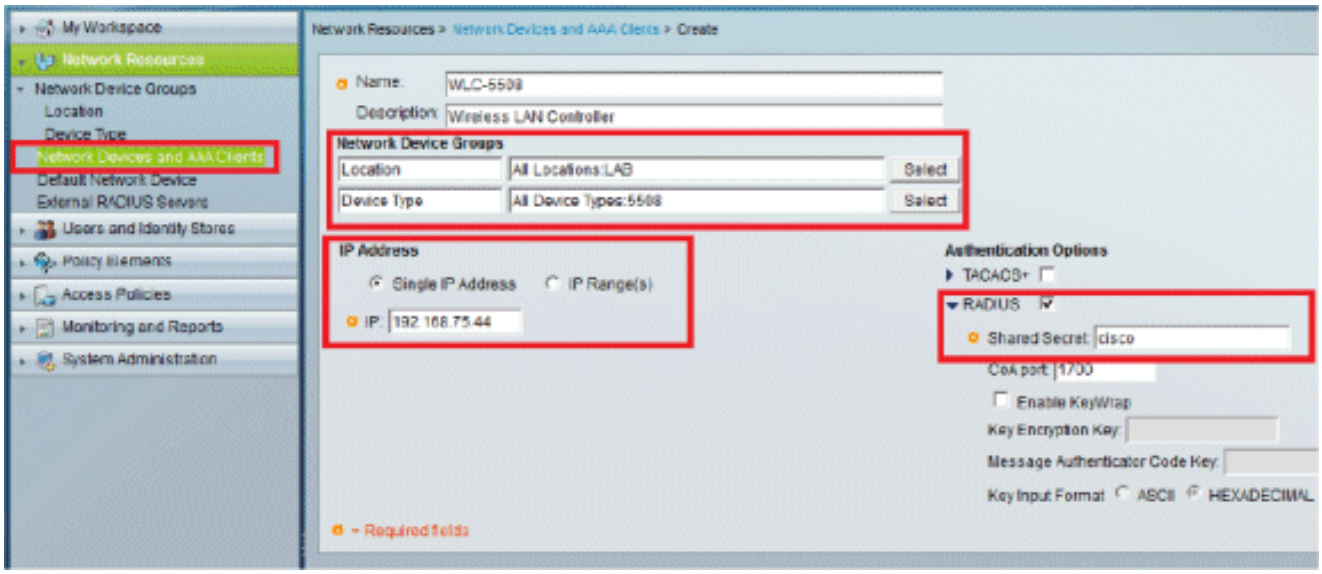
3. 单击Device Type > Create。



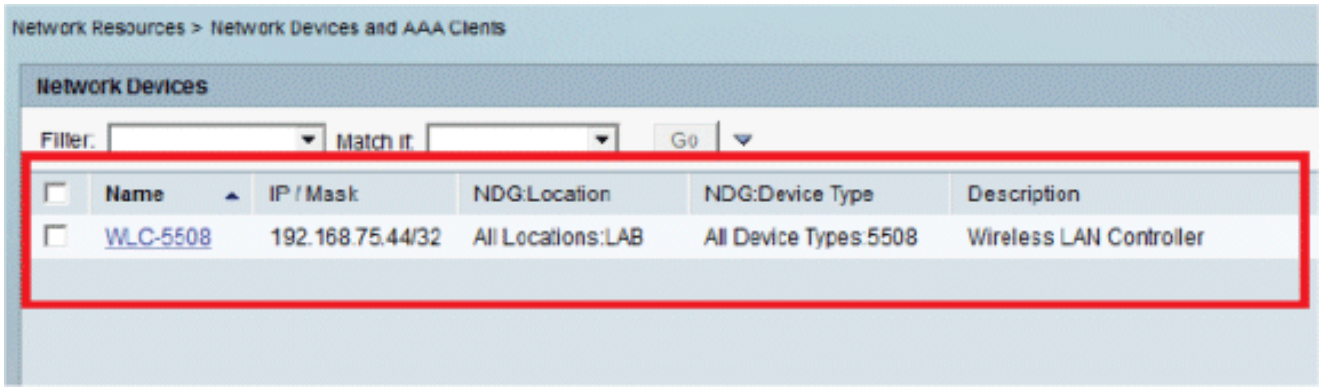
4. 单击“Submit”。现在您将看到以下屏幕：

5. 转至Network Resources > Network Devices and AAA Clients。

6. 单击Create，然后填写详细信息，如下所示：



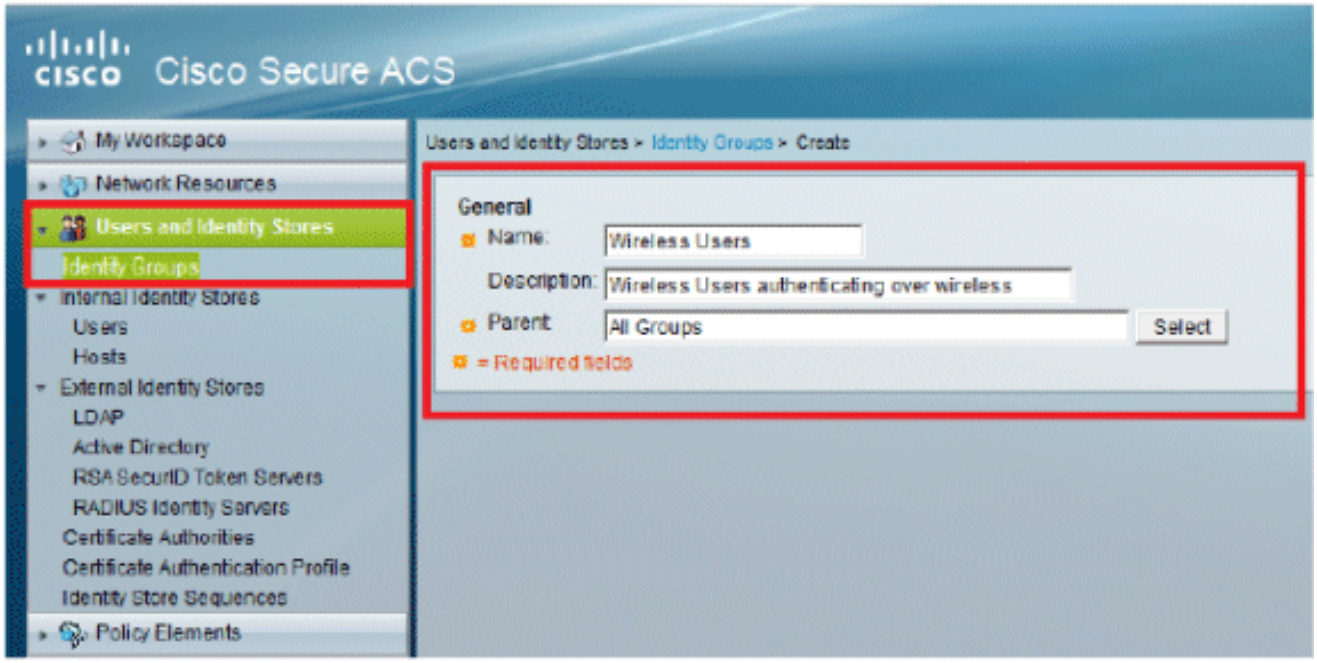
7. 单击“Submit”。现在您将看到以下屏幕：



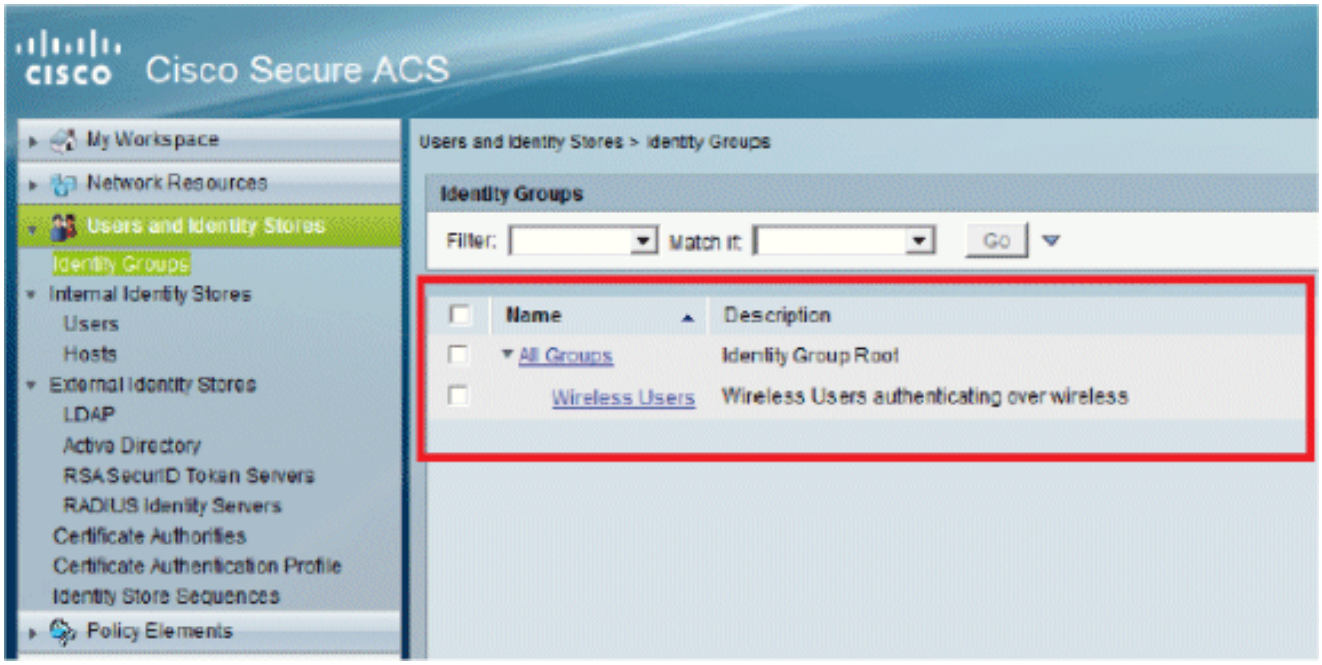
配置用户

在本节中，我们将在ACS上创建本地用户。用户（user1和user2）都分配到名为“无线用户”的组。

1. 转至Users and Identity Stores > Identity Groups > Create。

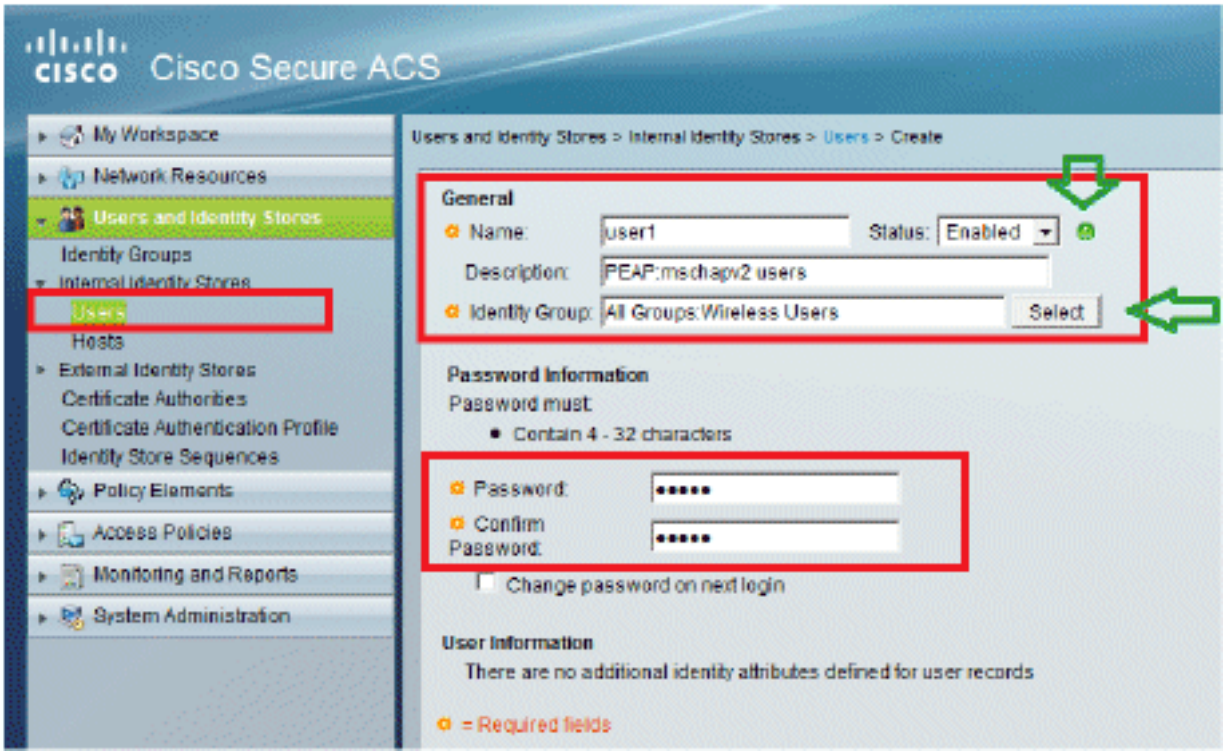


2. 单击Submit后，页面将如下所示：

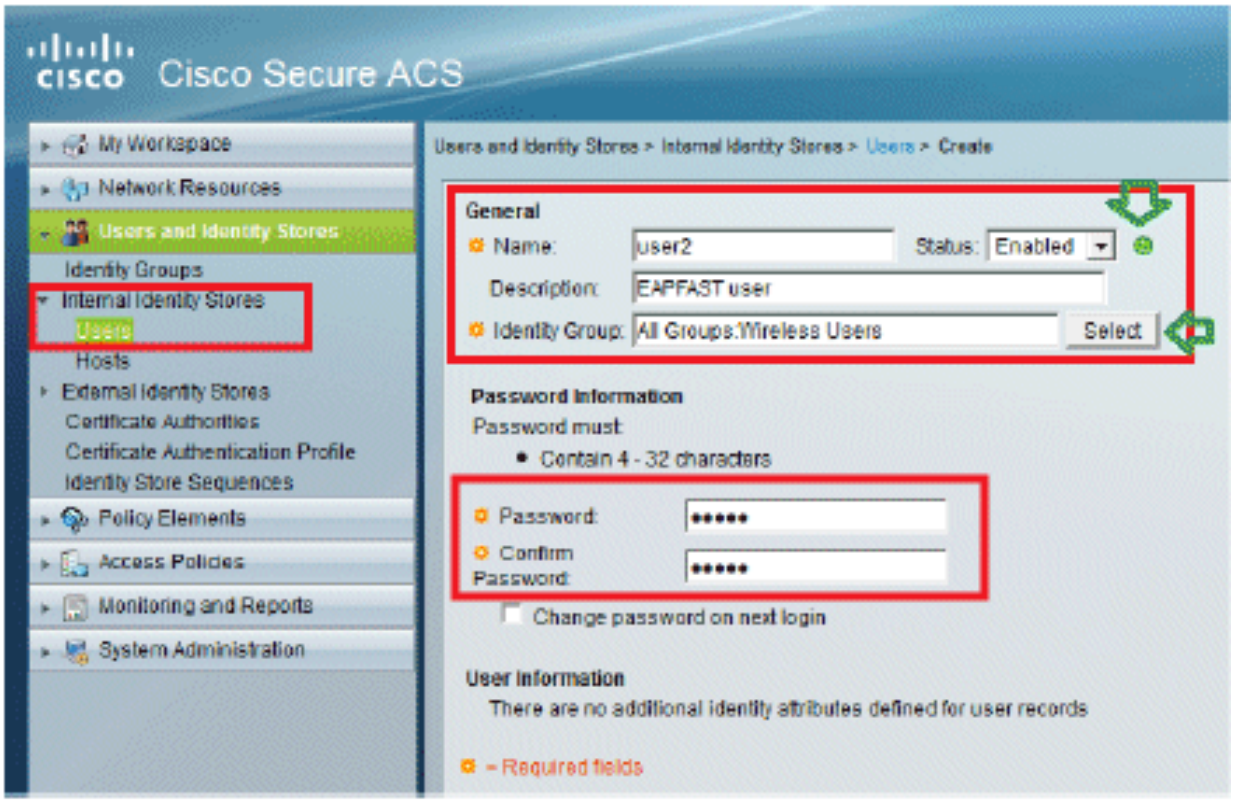


3. 创建用户user1和user2，并将它们分配到“Wireless Users”组。

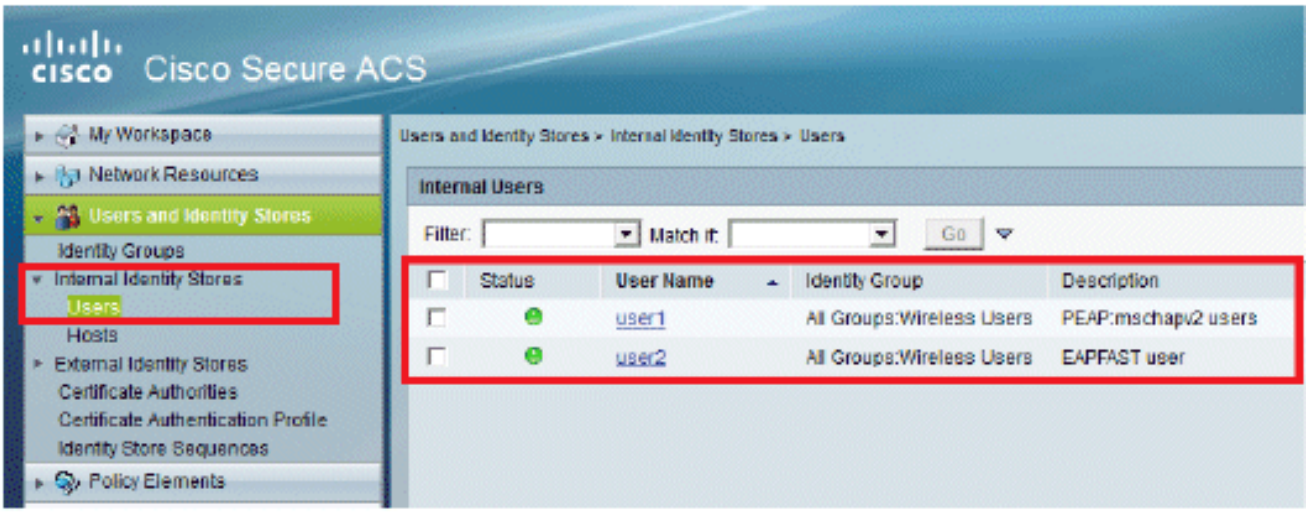
a. 单击Users and Identity Stores > Identity Groups > Users > Create。



b. 同样，创建user2。

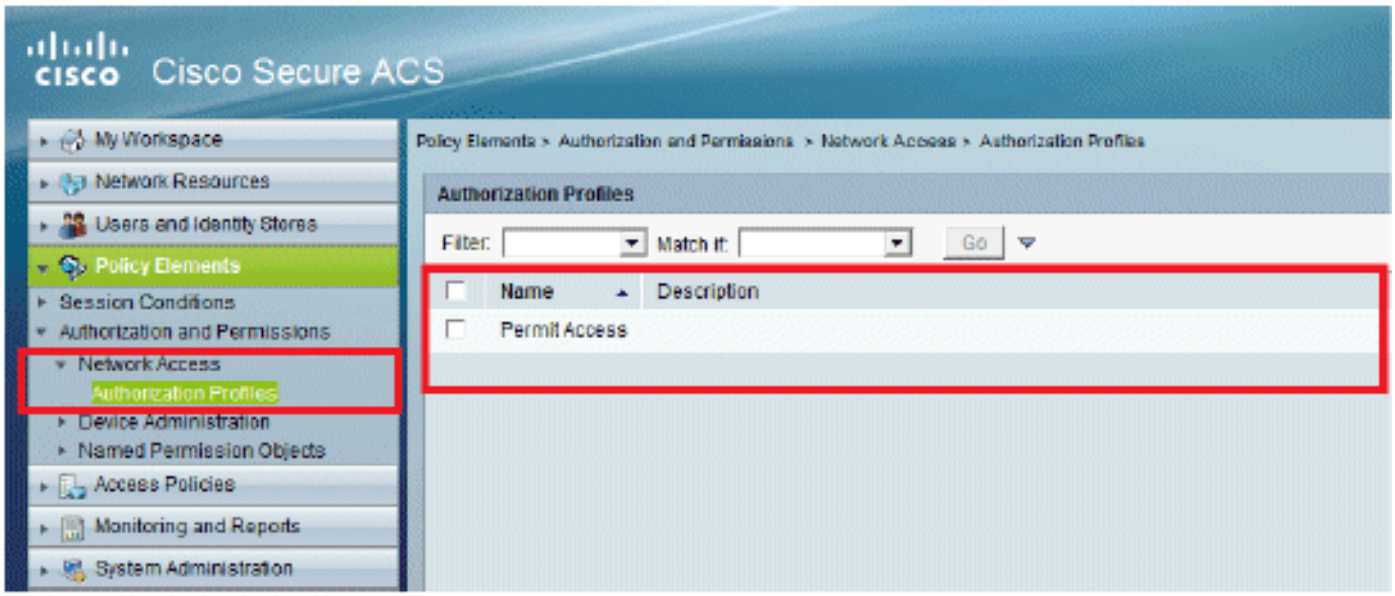


屏幕将如下所示：



定义策略元素

验证Permit Access已设置。

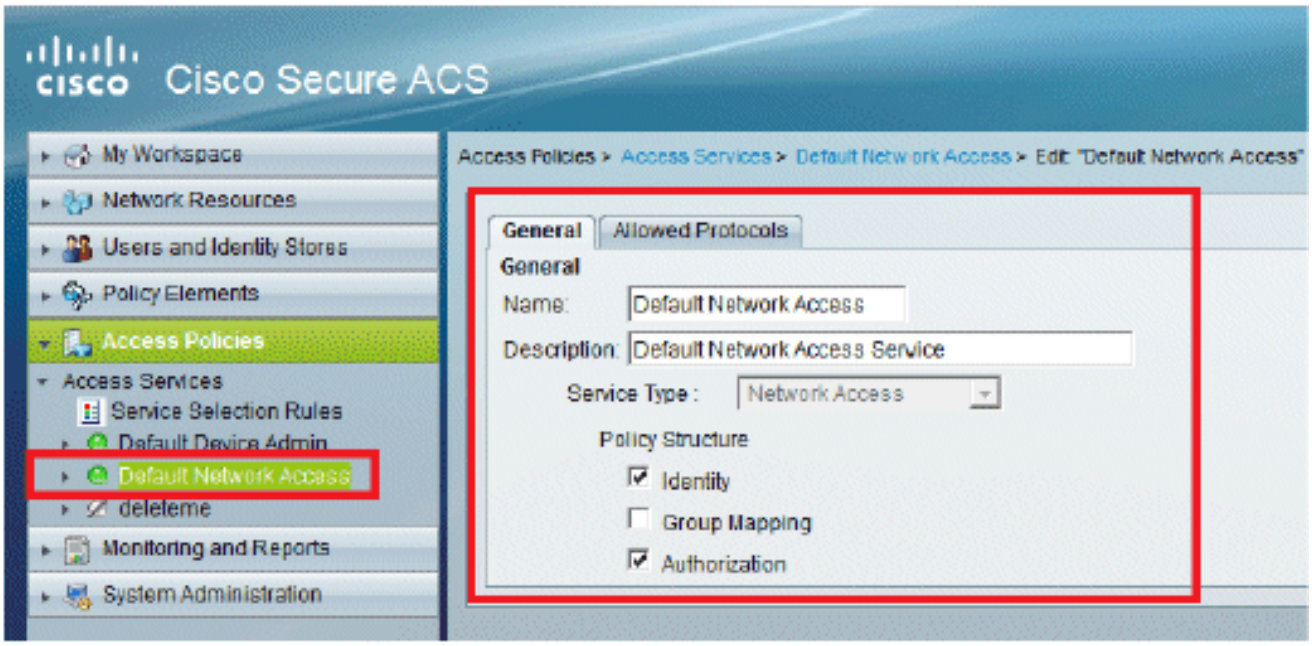


应用访问策略

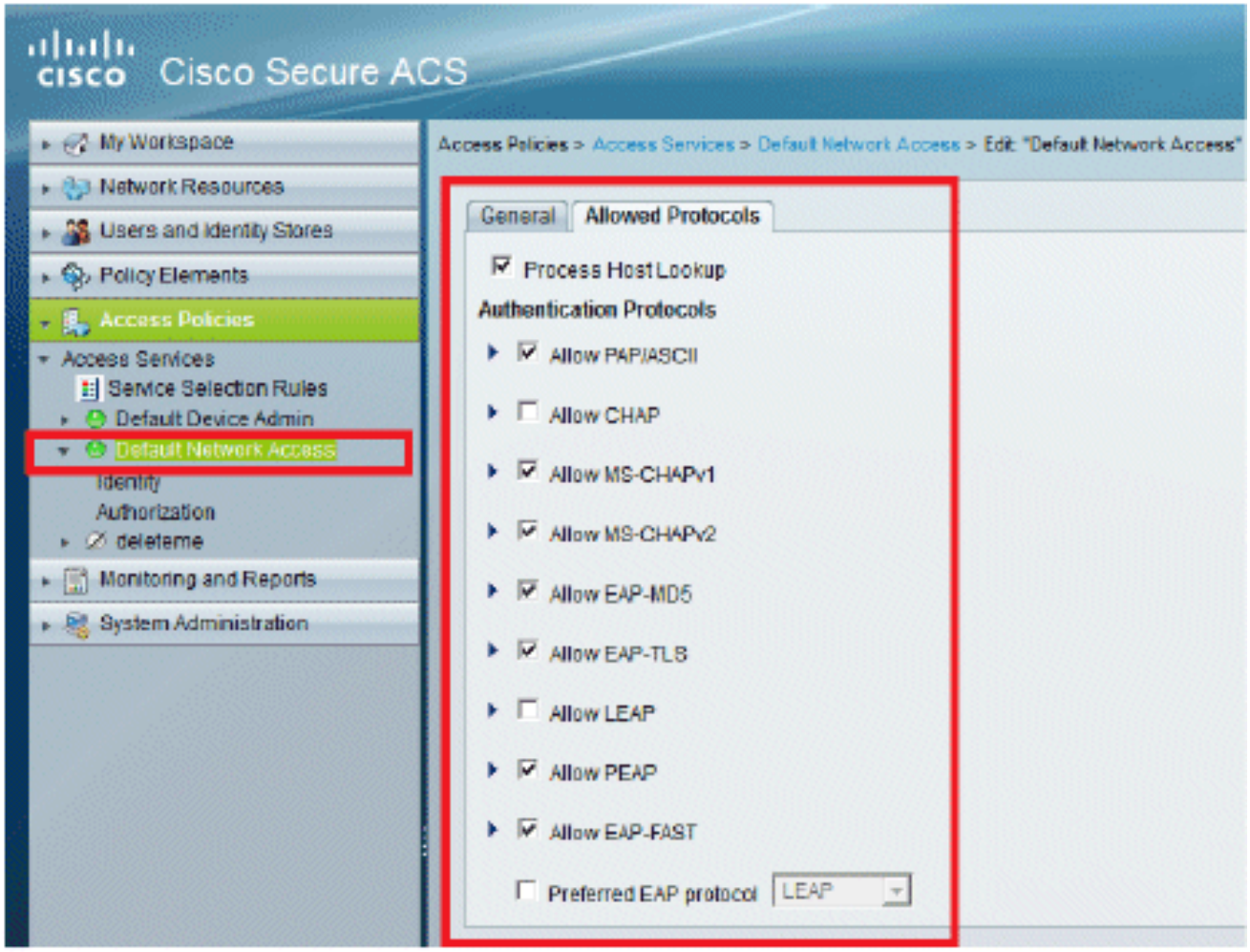
在本节中，我们将选择要使用的身份验证方法以及配置规则的方式。我们将根据前面的步骤创建规则。

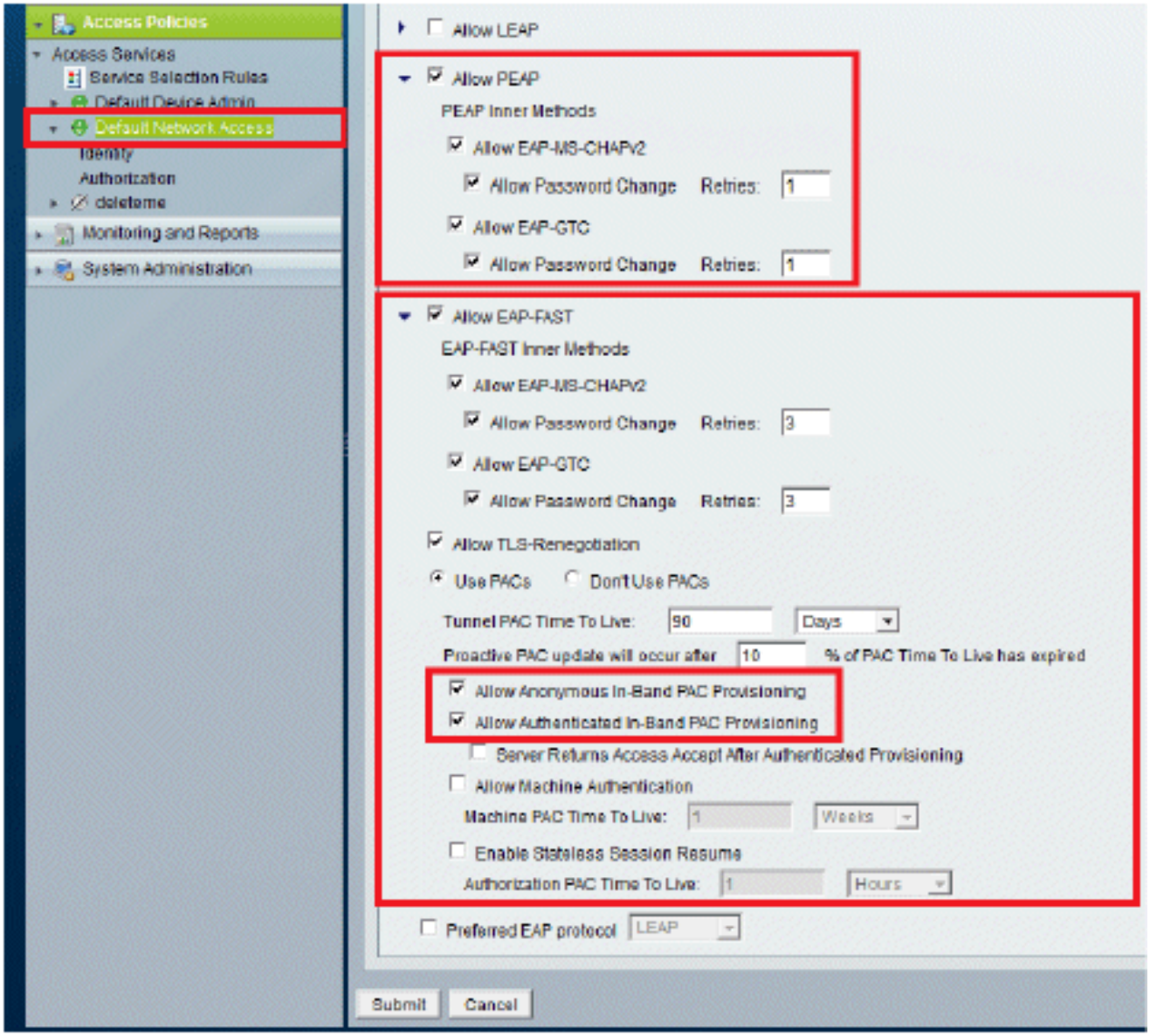
请完成以下步骤：

1. 转至Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"。



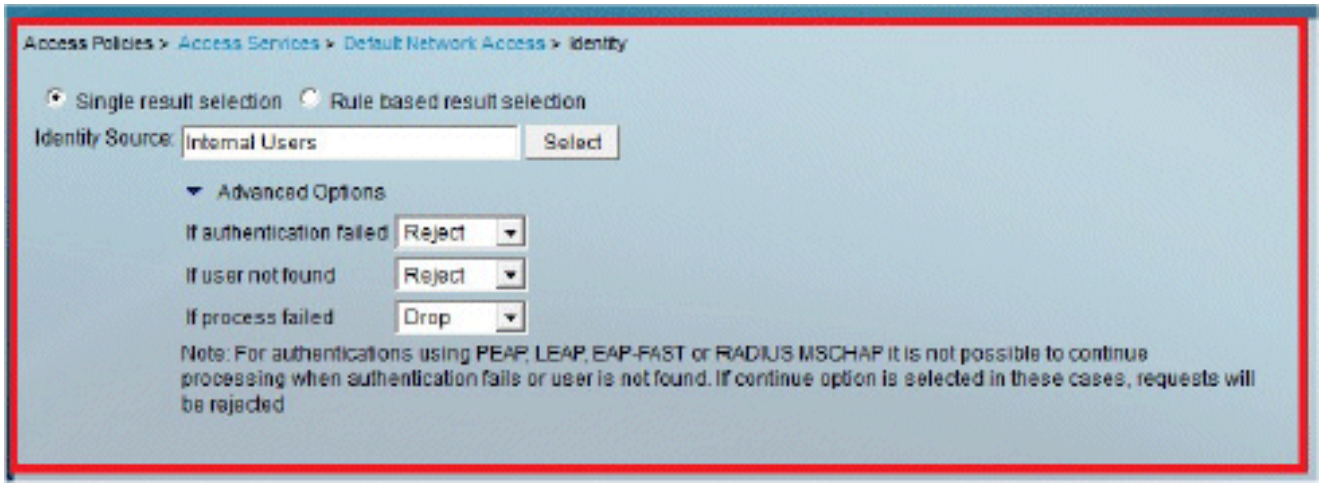
2. 选择您希望无线客户端进行身份验证的EAP方法。在本示例中，我们使用PEAP-MSCHAPv2和EAP-FAST。





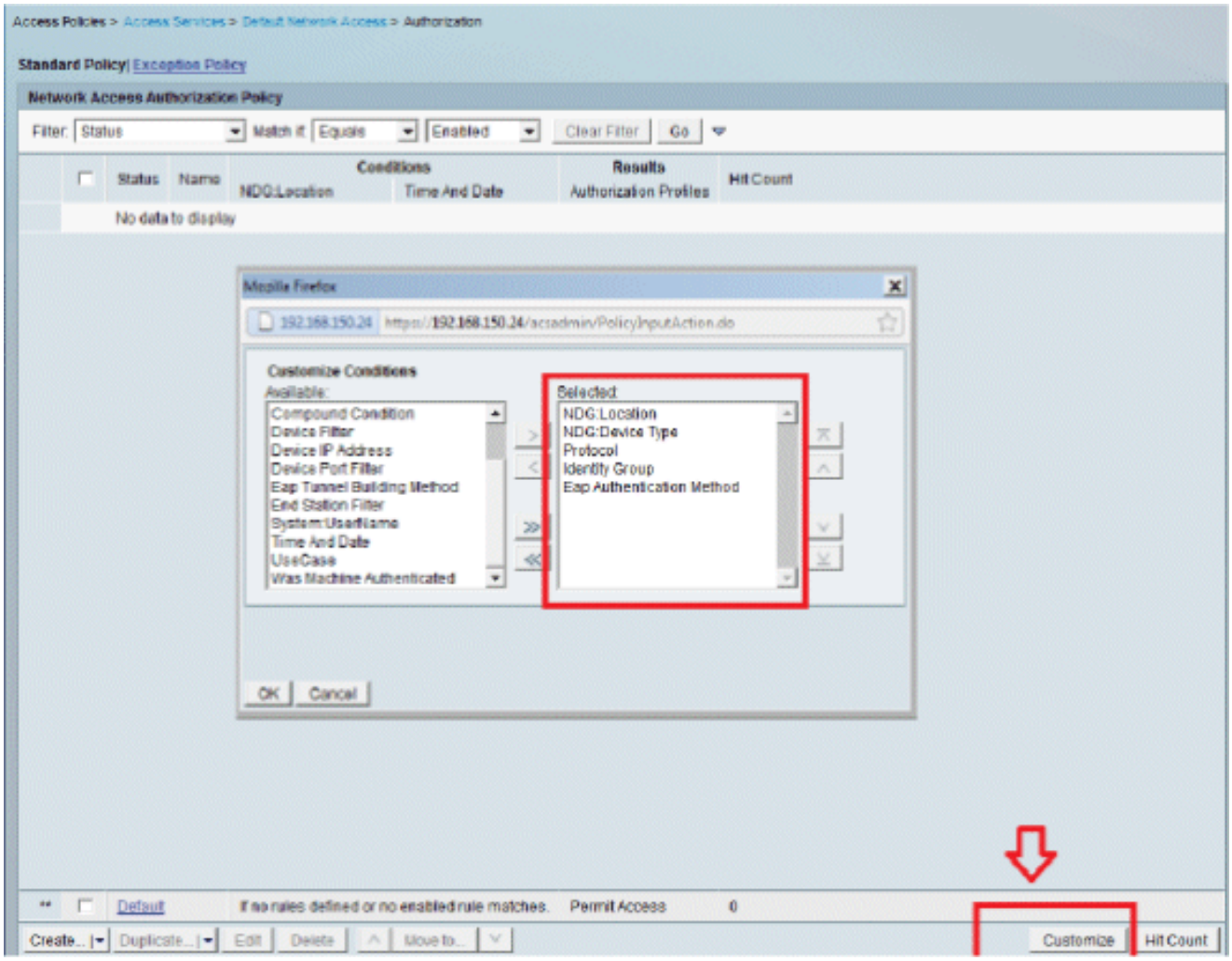
3. 单击“Submit”。

4. 验证您选择的身份组。在本示例中，我们使用Internal Users，这是我们在ACS上创建的。保存更改。



5. 要验证授权配置文件，请转到访问策略 > 访问服务 > 默认网络访问 > 授权。

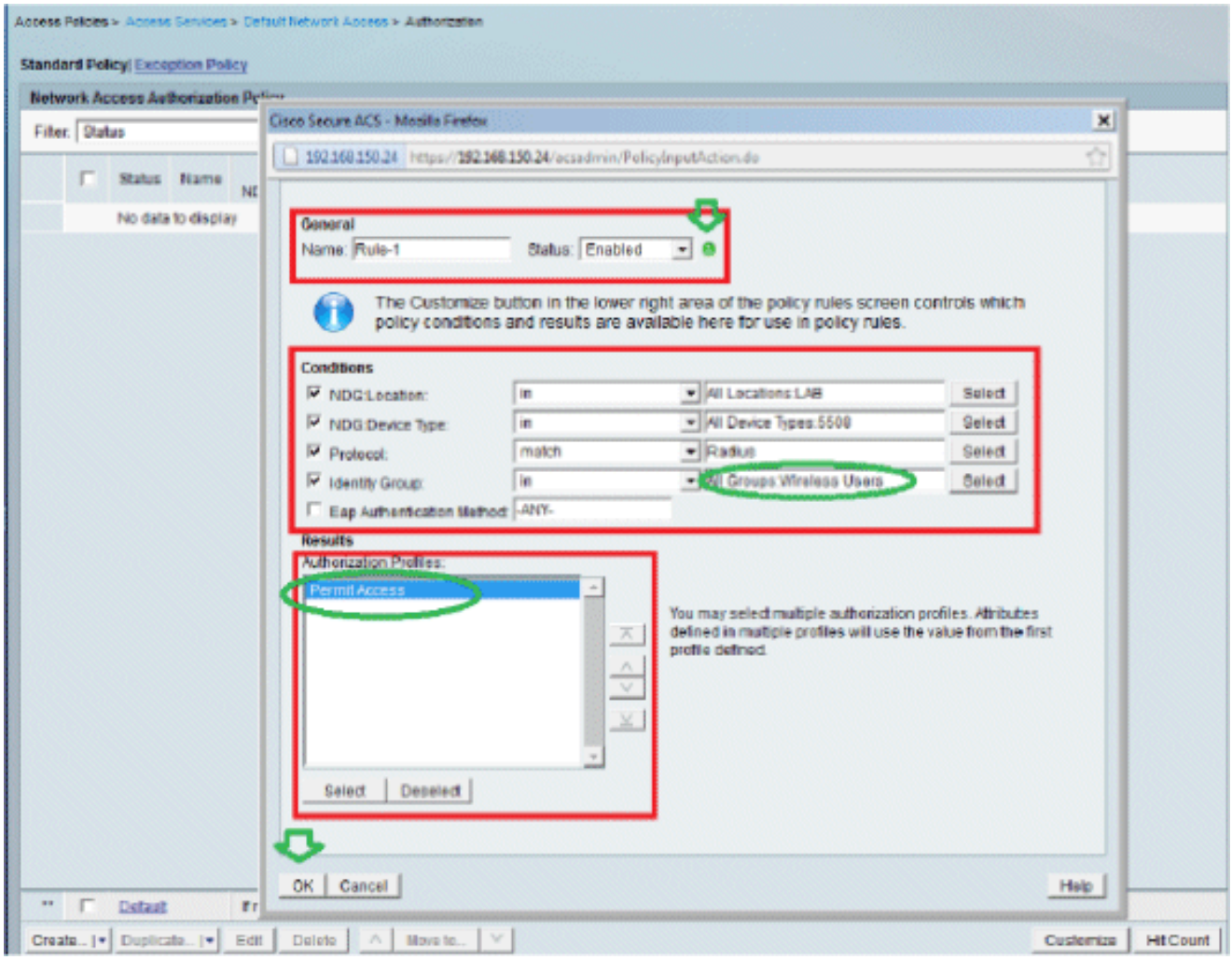
您可以自定义在什么条件下允许用户访问网络，以及经过身份验证后通过什么授权配置文件（属性）。此精细度仅在ACS 5.x中可用。在本示例中，我们选择Location、Device Type、Protocol、Identity Group和EAP Authentication Method。



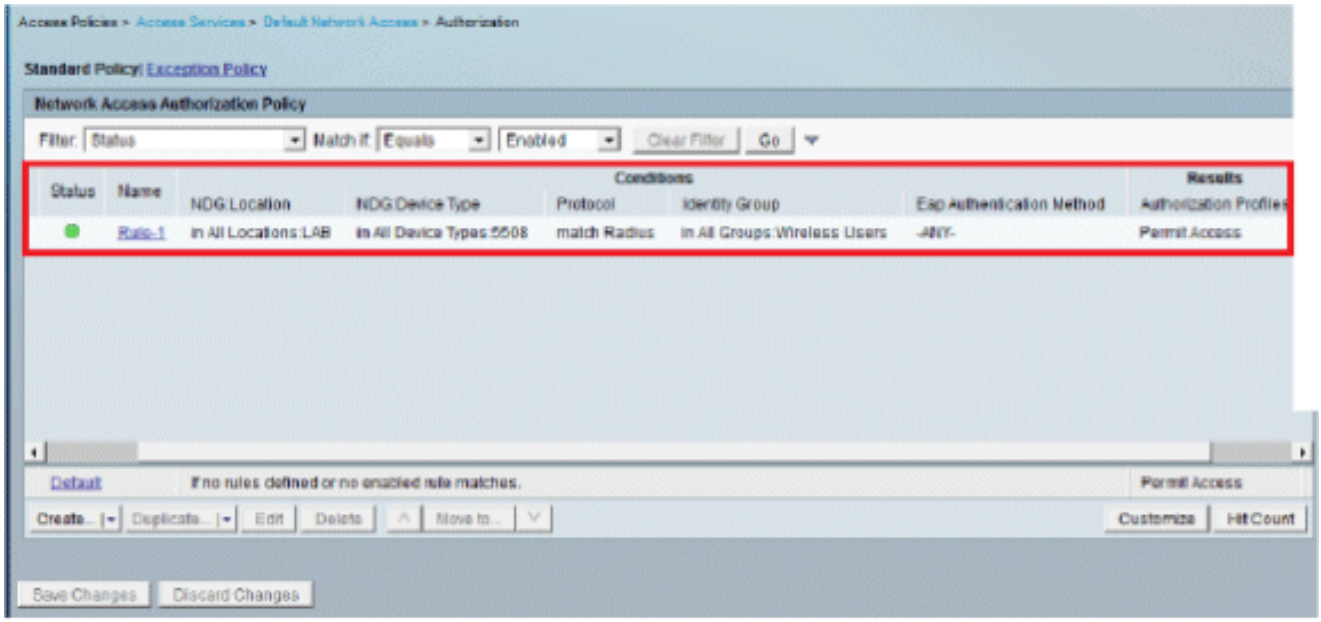
6. 单击确定，然后单击保存更改。

7. 下一步是创建规则。如果未定义规则，则允许客户端在不带任何条件的情况下访问。

   单击Create > Rule-1。此规则适用于“无线用户”组中的用户。

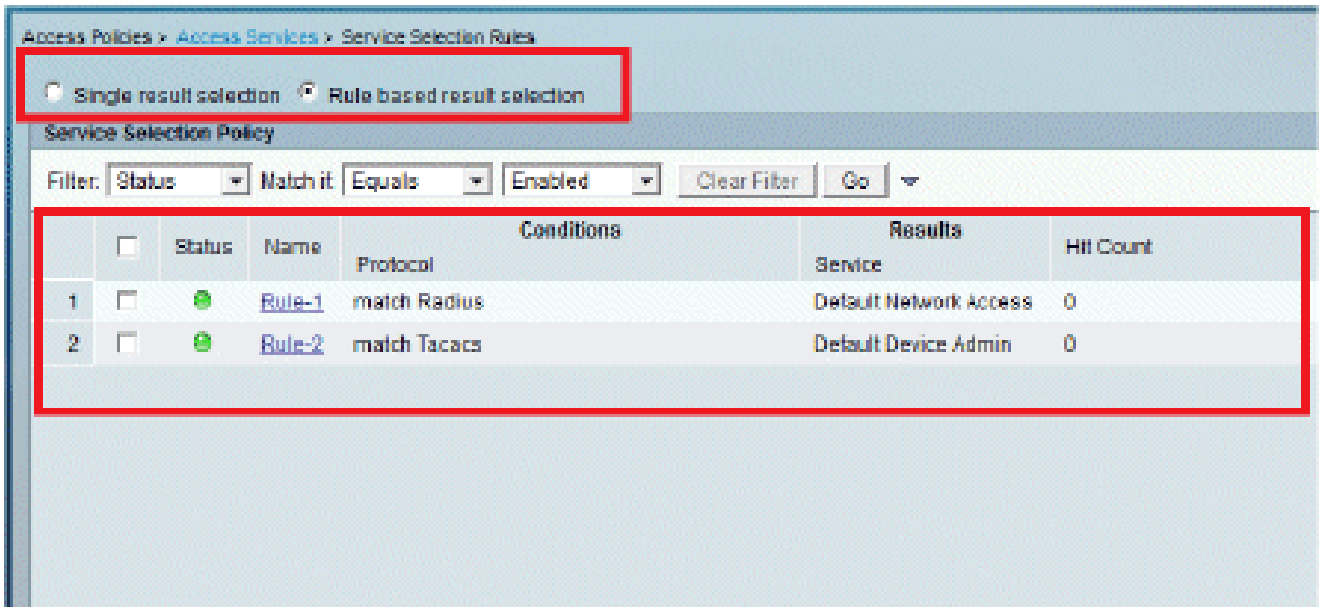


8. 保存更改。屏幕将如下所示：



如果希望拒绝不匹配条件的用户，请编辑默认规则以显示“拒绝访问”。

9. 现在我们将定义服务选择规则。使用此页可以配置简单策略或基于规则的策略，以确定将哪种服务应用于传入请求。在本示例中，使用基于规则的策略。



配置 WLC

此配置要求执行下列步骤：

1. 用身份验证服务器的详细信息配置 WLC.
2. 配置动态接口(VLAN)。
3. 配置WLAN(SSID)。

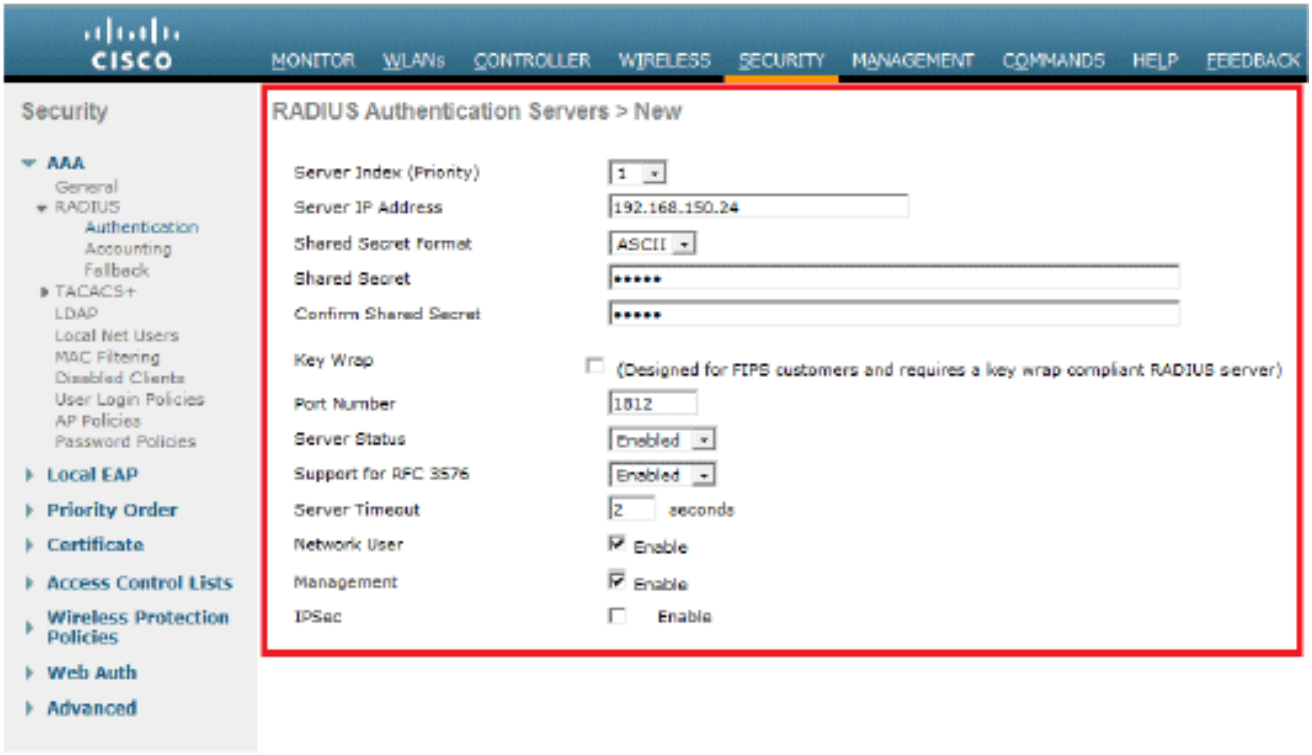
用身份验证服务器的详细信息配置 WLC

必须配置WLC，使其可以与RADIUS服务器进行通信，以便对客户端进行身份验证，以及执行任何其他事务。

请完成以下步骤：

1. 从控制器 GUI 中，单击 Security。
2. 输入 RADIUS 服务器的 IP 地址以及在 RADIUS 服务器和 WLC 之间使用的共享密钥。

   此共享密钥应与RADIUS服务器中配置的密钥相同。

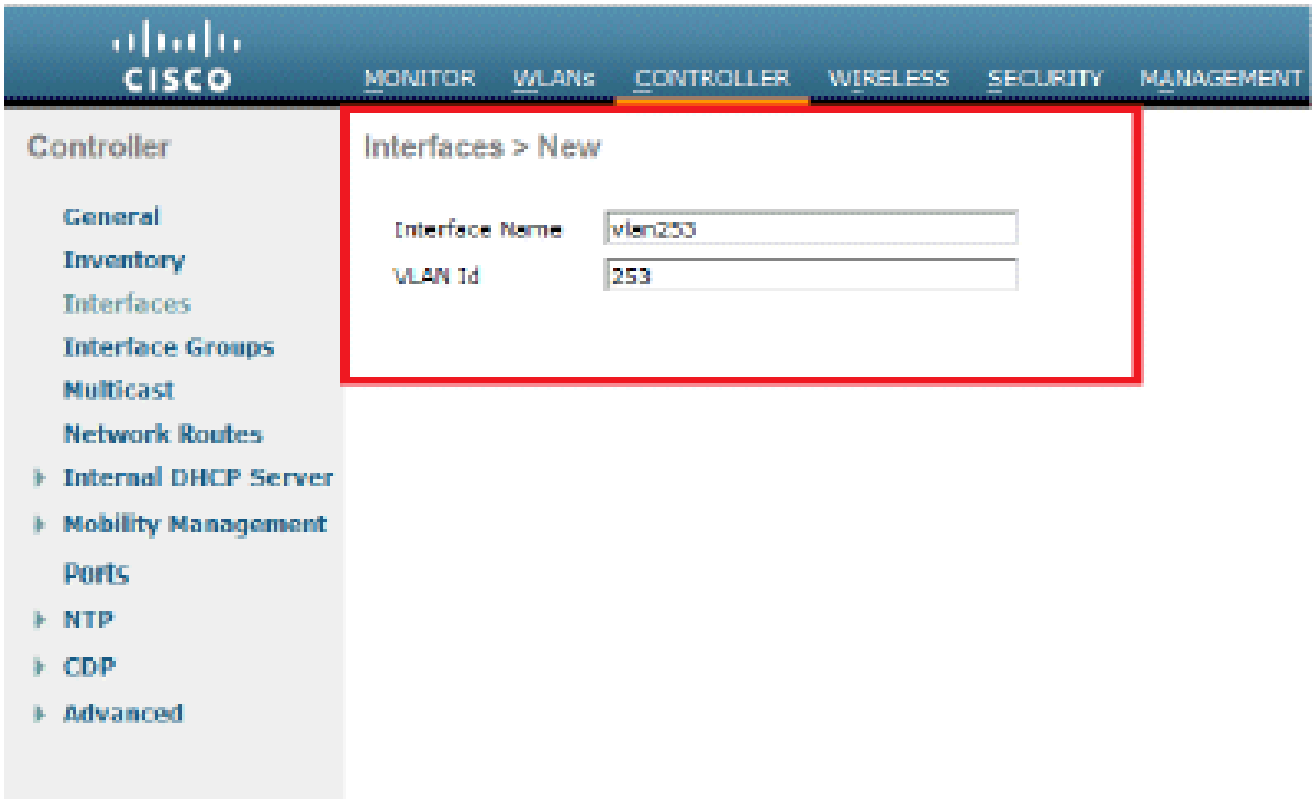


配置动态接口 (VLAN)

此过程介绍如何在WLC上配置动态接口。

请完成以下步骤：

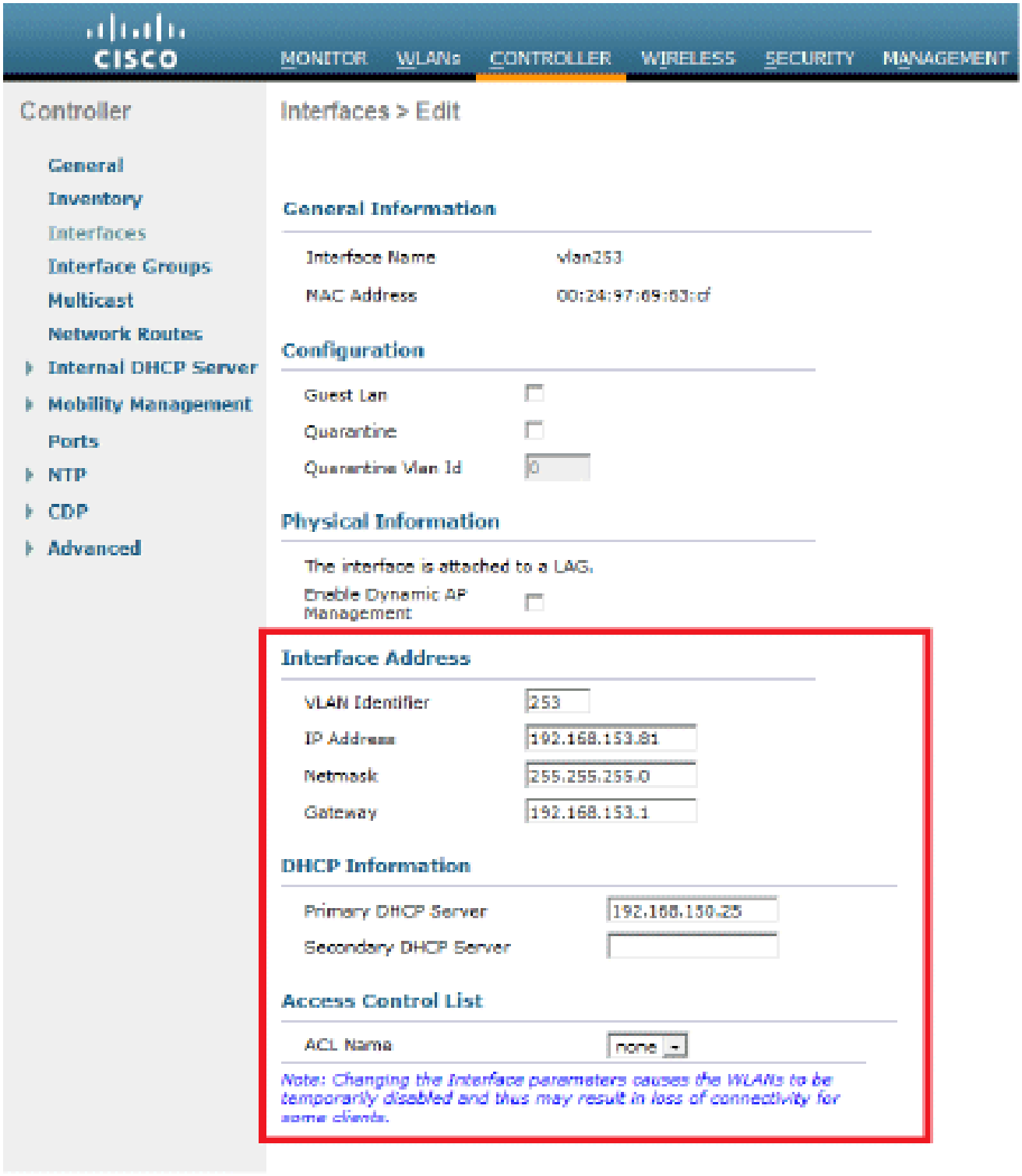
1. 动态接口是在控制器GUI的Controller > Interfaces窗口中配置的。



2. 单击 Apply。

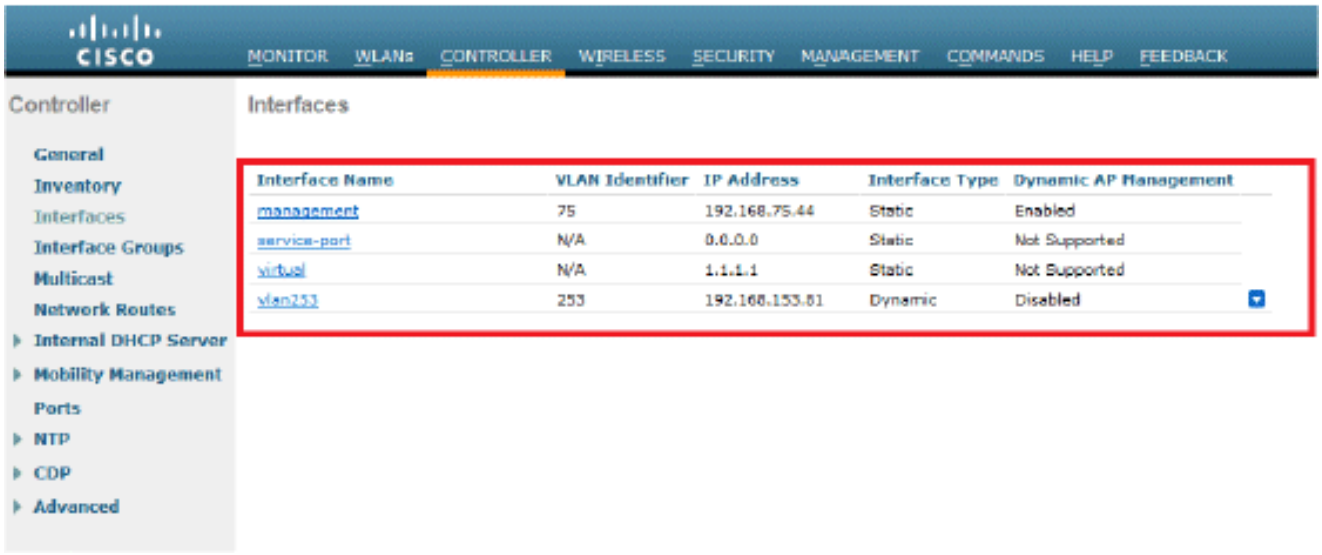
   这会将您带到此动态接口（这里为 VLAN 253）的 Edit 窗口中。

3. 输入此动态接口的 IP 地址和默认网关。



4. 单击 Apply。

5. 配置的接口如下所示：



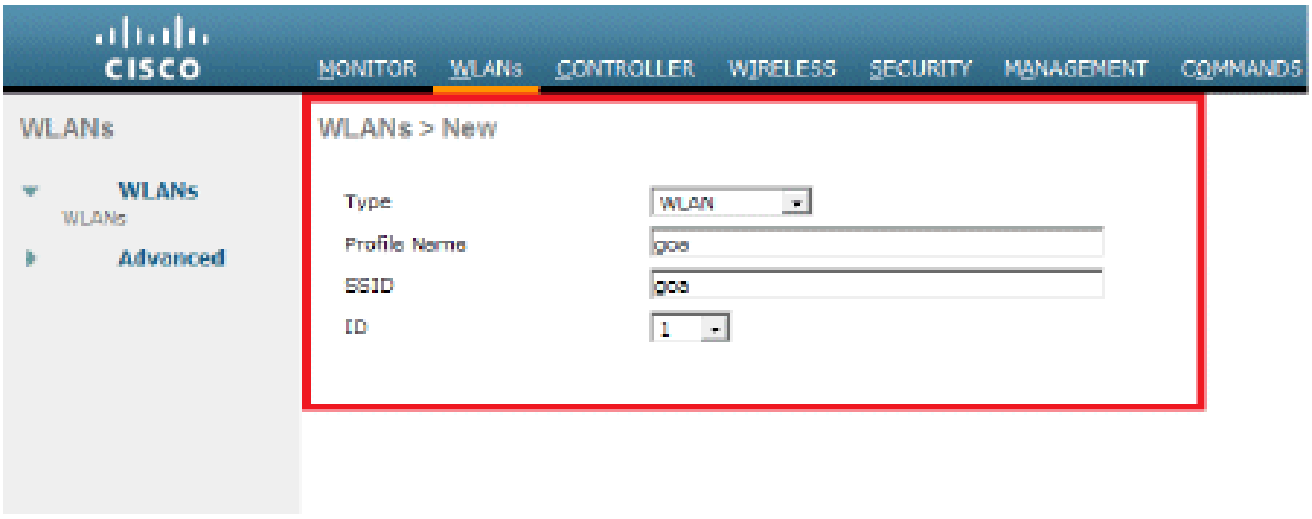
配置 WLAN (SSID)

此过程说明如何在 WLC 中配置 WLAN。

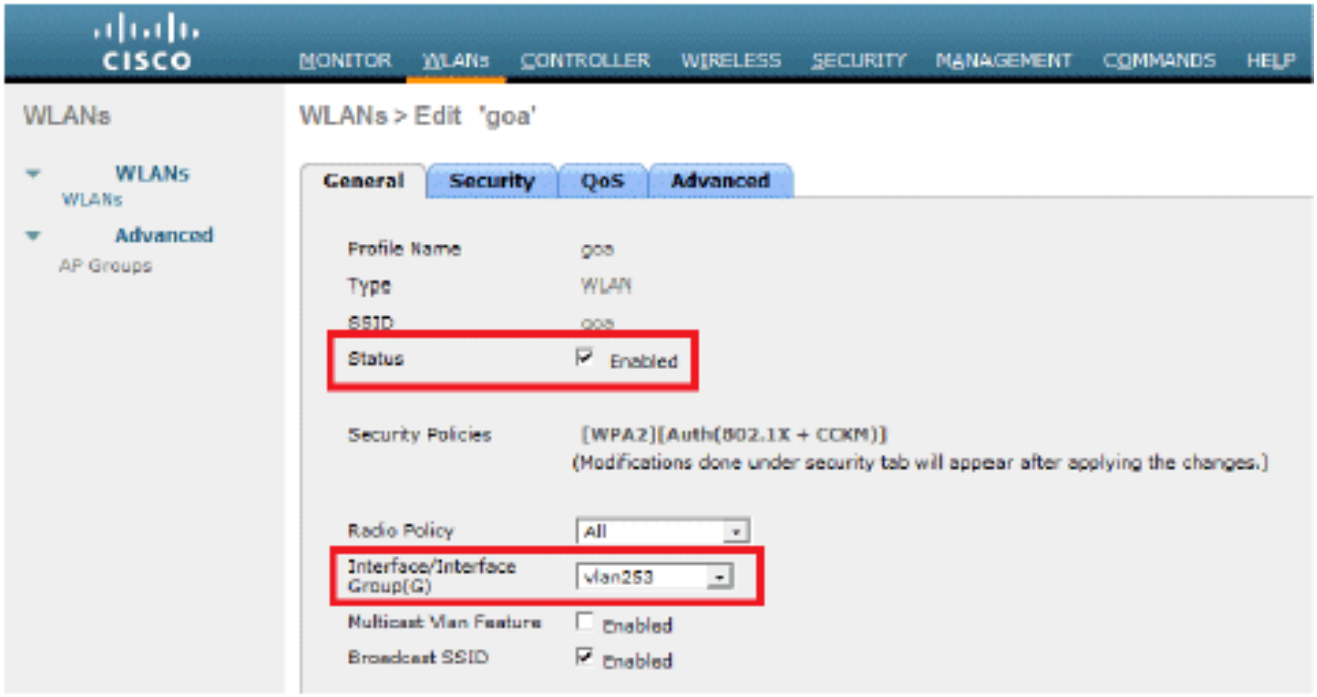
请完成以下步骤：

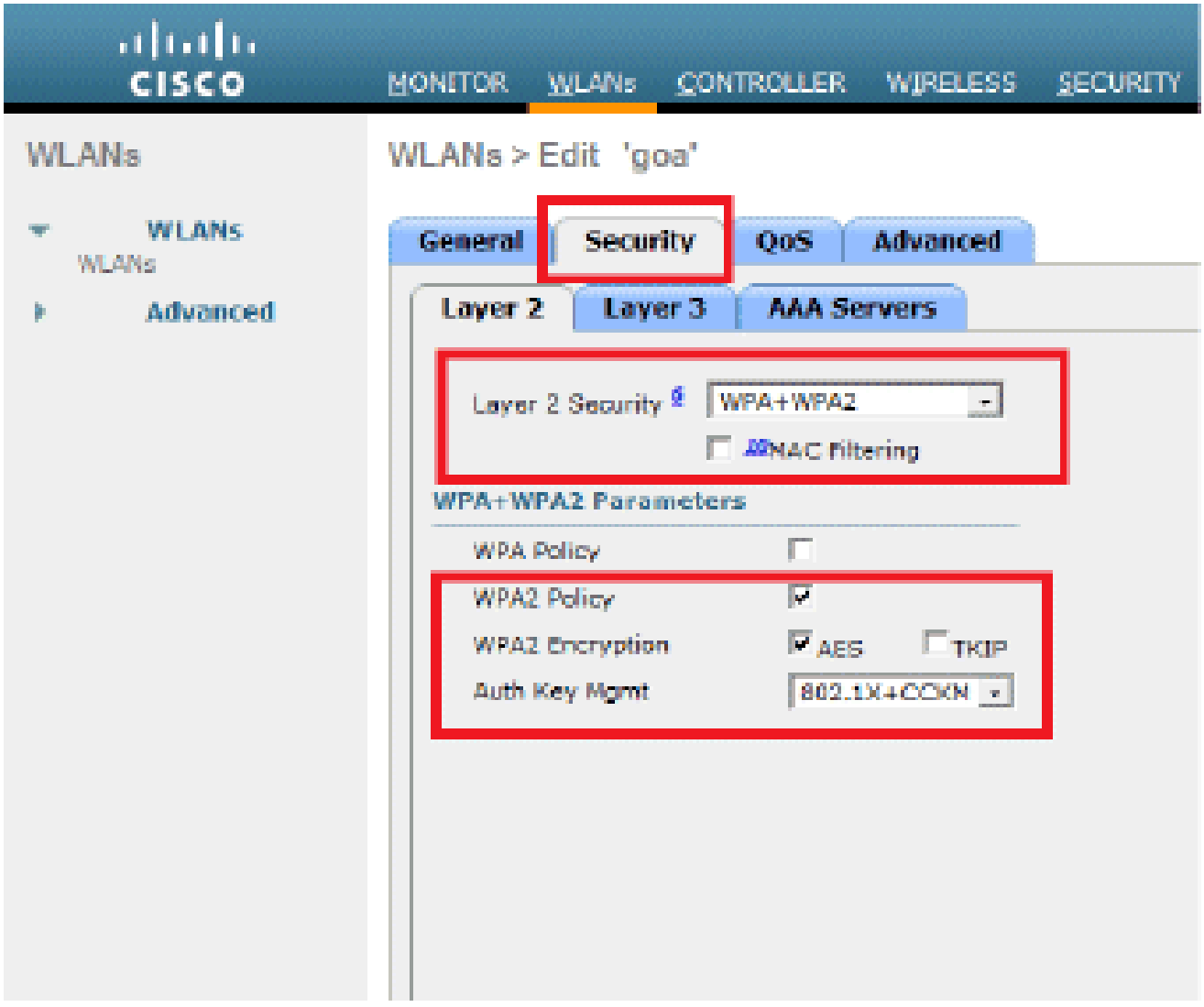
1. 从控制器GUI中，转到WLANs > Create New以创建新的WLAN。此时会显示 New WLANs 窗口。
2. 输入 WLAN ID 和 WLAN SSID 信息。

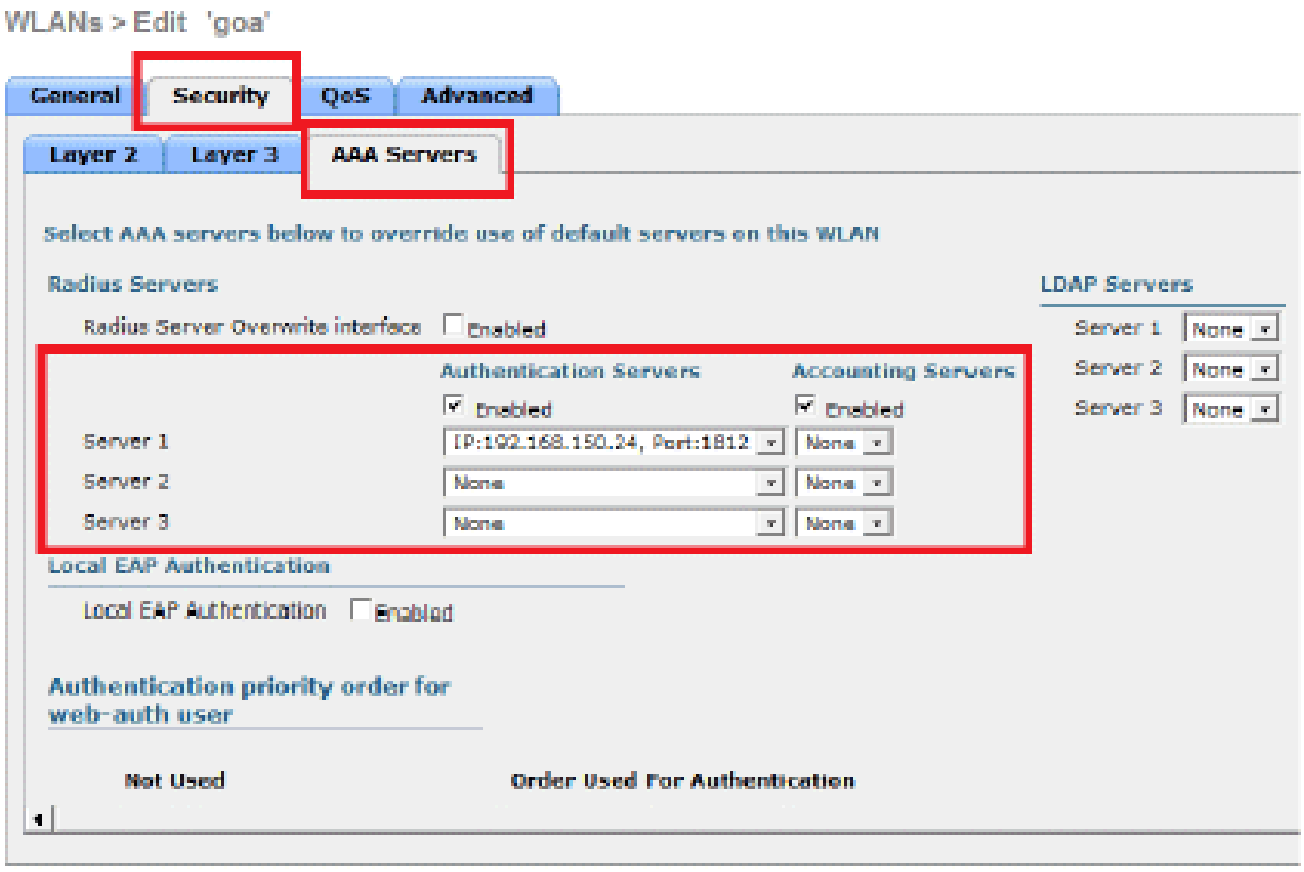
   您可以输入任何名称作为WLAN SSID。本示例使用goa作为WLAN SSID。

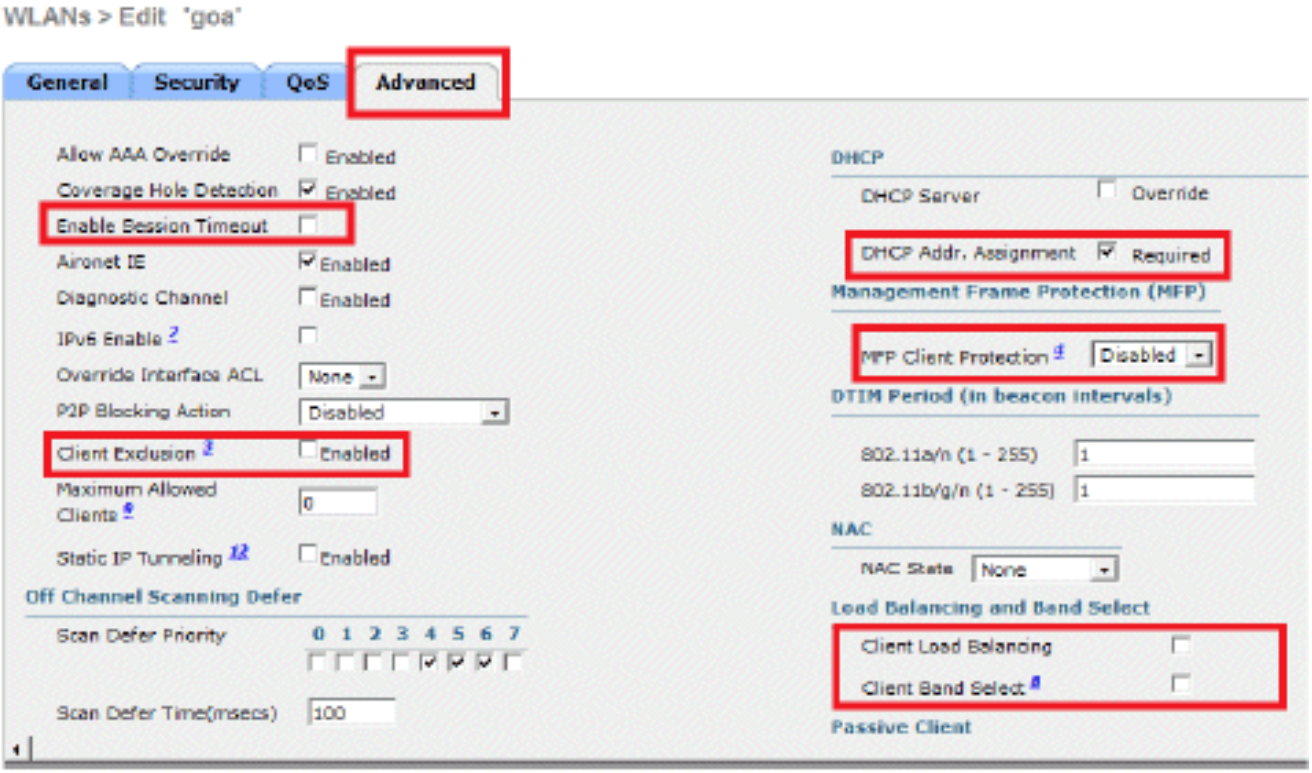


3. 单击Apply以转到WLAN目标的Edit窗口。


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
Advanced
AP Groups
WLANs > Edit 'goa'
General Security QoS Advanced
Profile Name goa
Type WLAN
SSID goa
Status Enabled
Security Policies [WPA2][Auth(802.1X + CCKM)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy All
Interface/Interface Group(G) vlan253
Multicast Vlan Feature Enabled
Broadcast SSID Enabled


CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY
WLANs
WLANs
WLANs
Advanced
WLANs > Edit 'goa'
General Security QoS Advanced
Layer 2 Layer 3 AAA Servers
Layer 2 Security WPA+WPA2
MAC Filtering
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption AES TKIP
Auth Key Mgmt 802.1X+CCKM





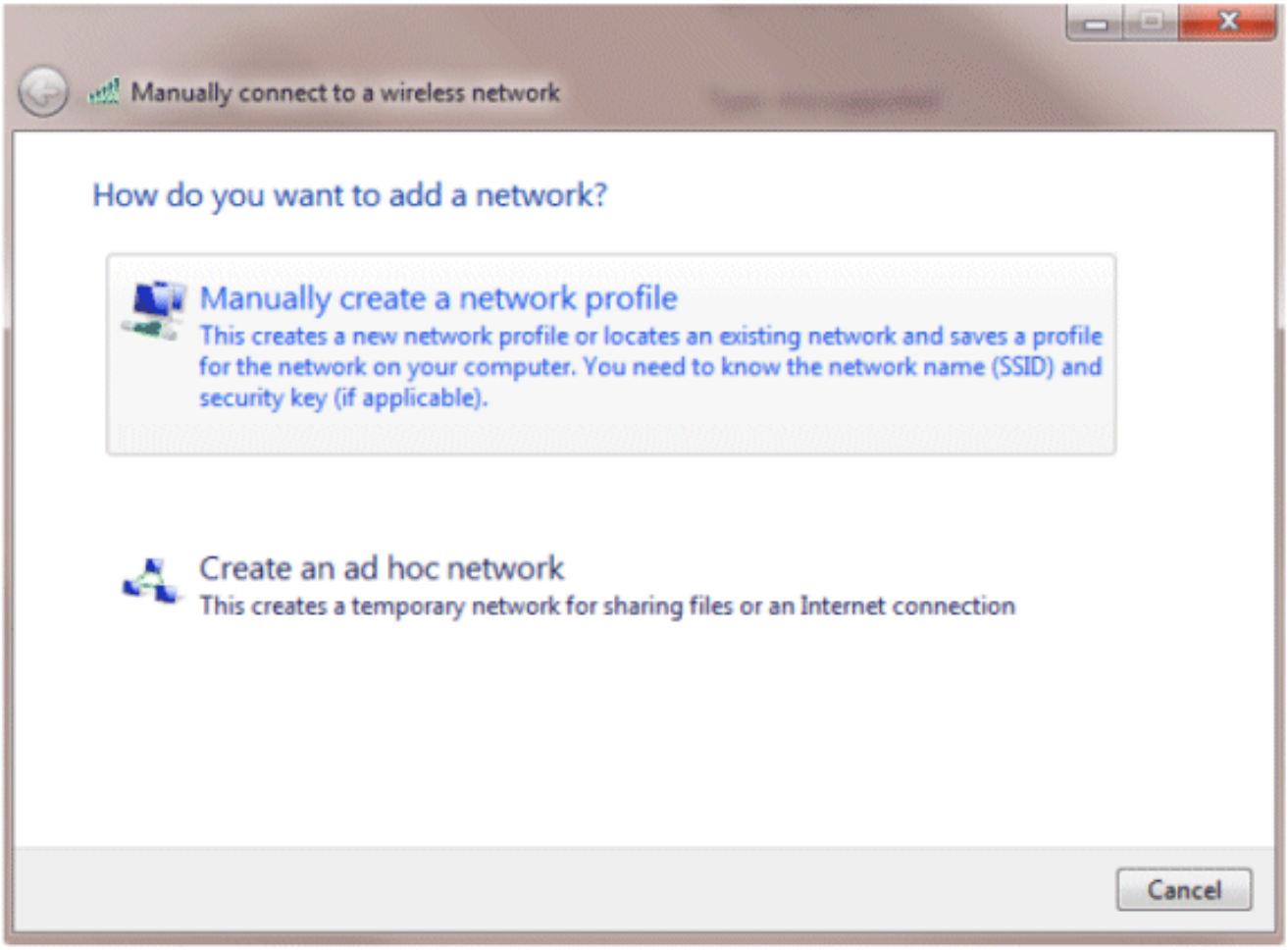
配置无线客户端实用程序

PEAP-MSCHAPv2(user1)

在我们的测试客户端中，我们使用的是运行14.3驱动程序版本的Intel 6300-N卡的Windows 7原生Supplicant客户端。建议使用供应商提供的最新驱动程序进行测试。

要在Windows零配置(WZC)中创建配置文件，请完成以下步骤：

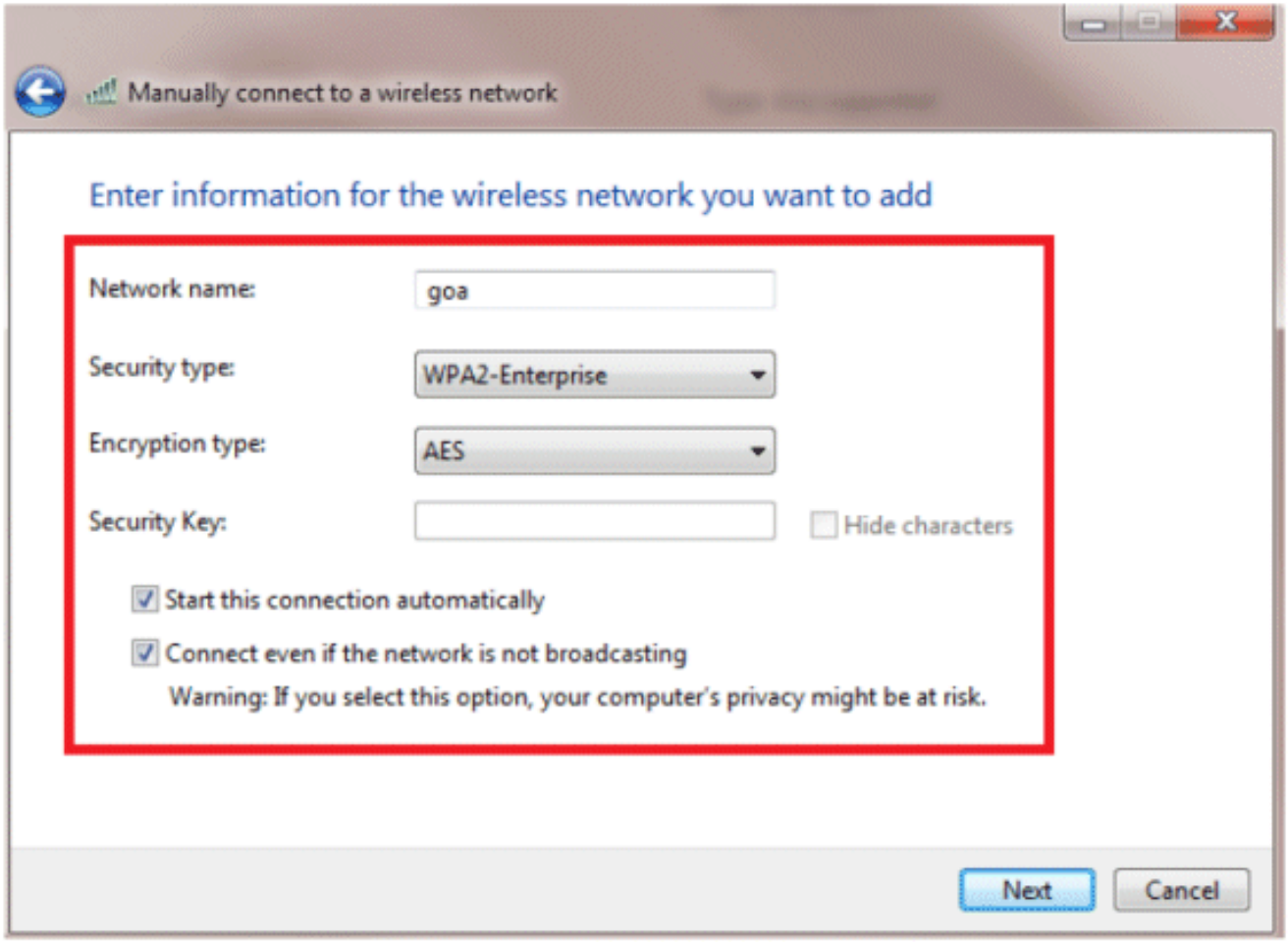
1. 转至控制面板 > 网络和Internet > 管理无线网络。
2. 单击Add选项卡。
3. 单击Manually create a network profile。



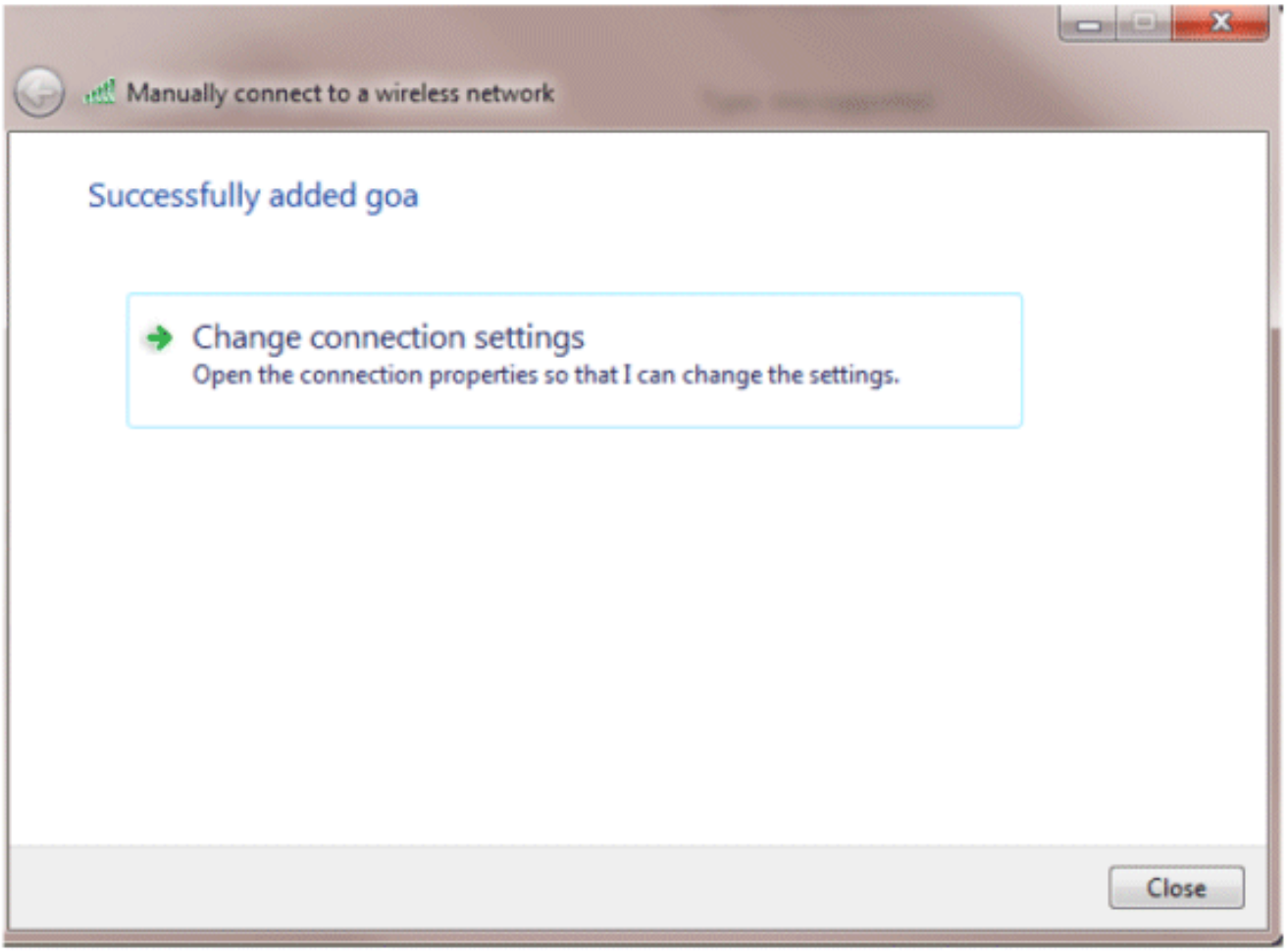
4. 添加在WLC上配置的详细信息。

   注意：SSID区分大小写。

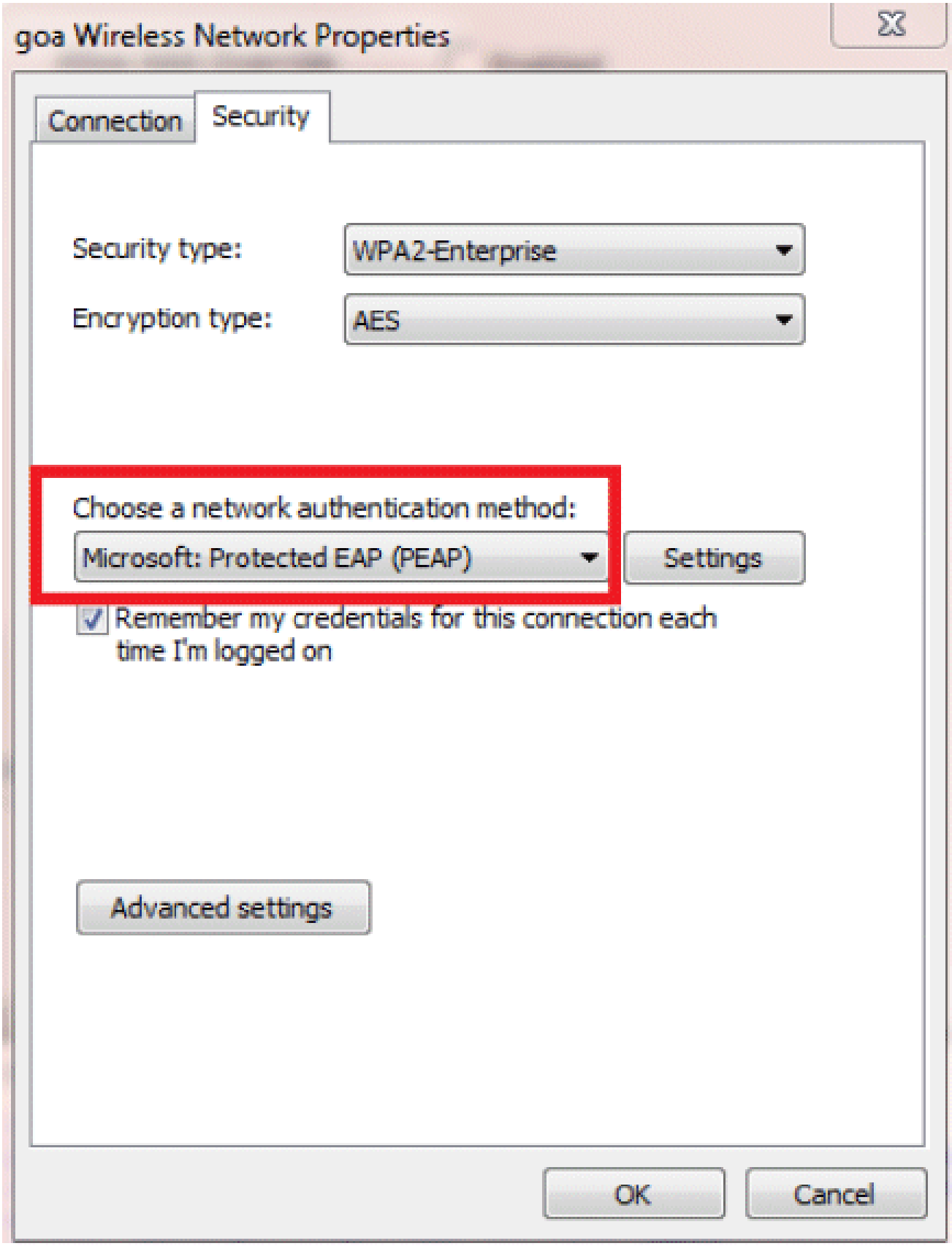
5. 单击 Next。

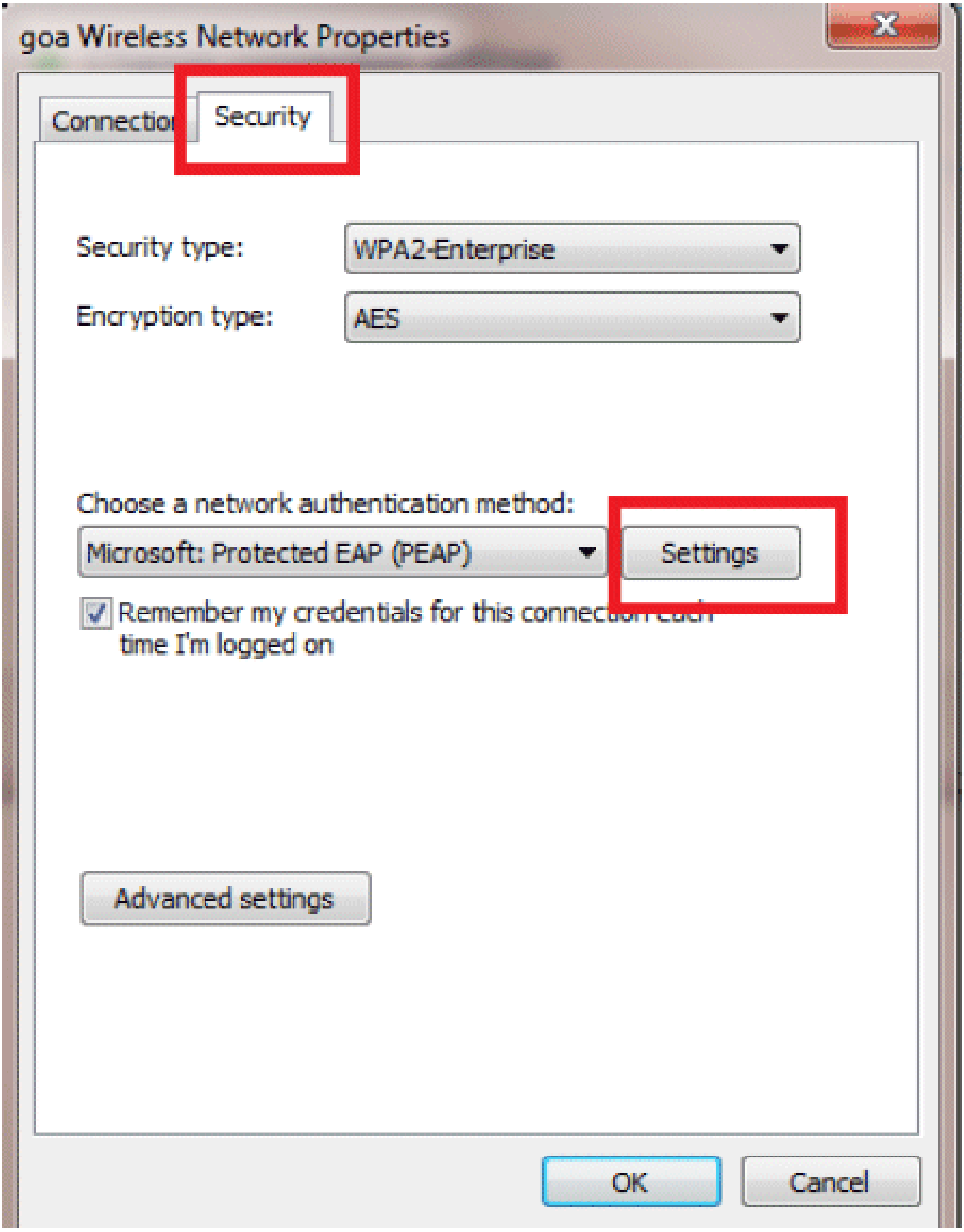


6. 单击Change connection settings以仔细检查设置。

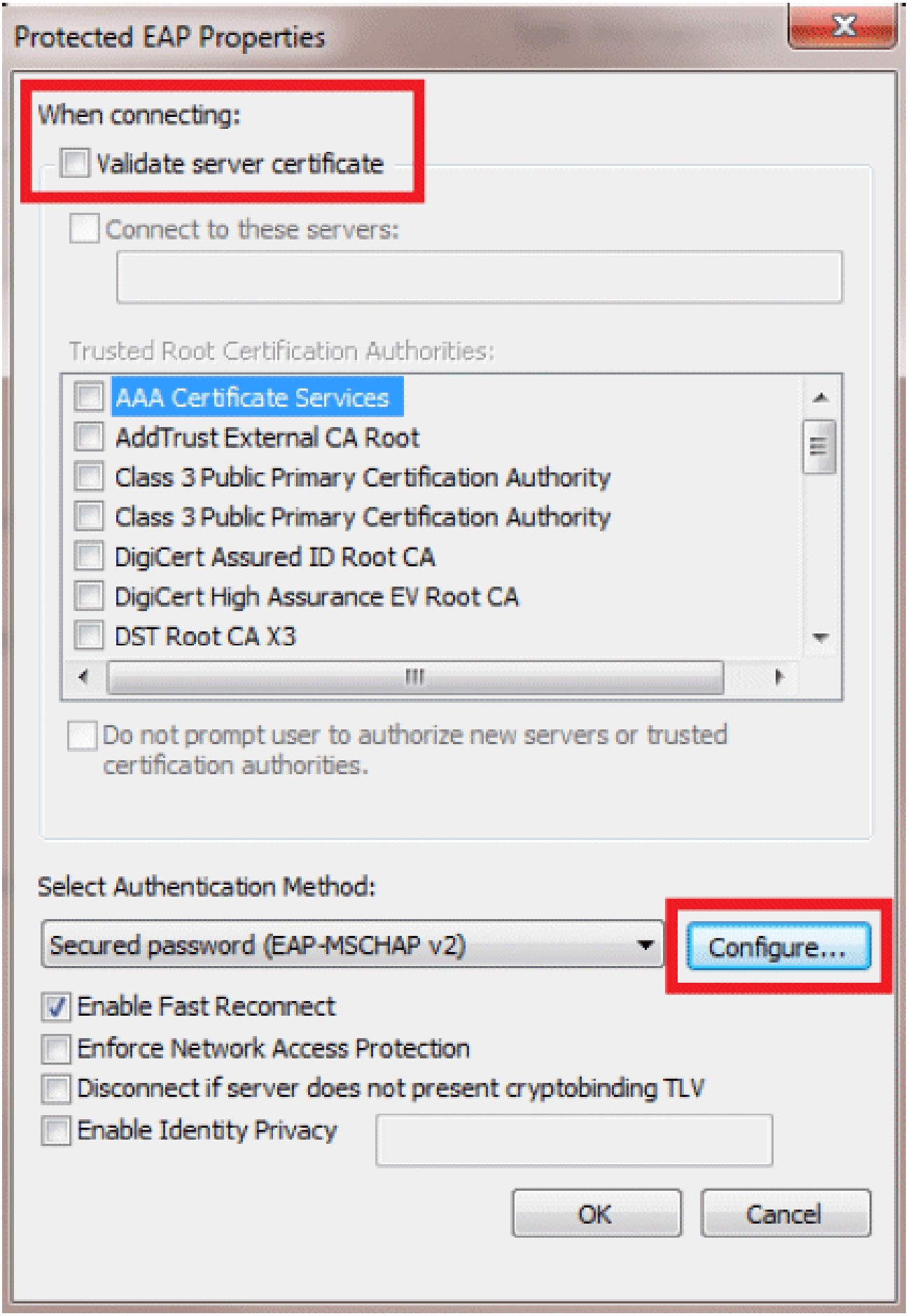

Manually connect to a wireless network
Successfully added goa
Change connection settings
Open the connection properties so that I can change the settings.
Close

7. 确保已启用PEAP。

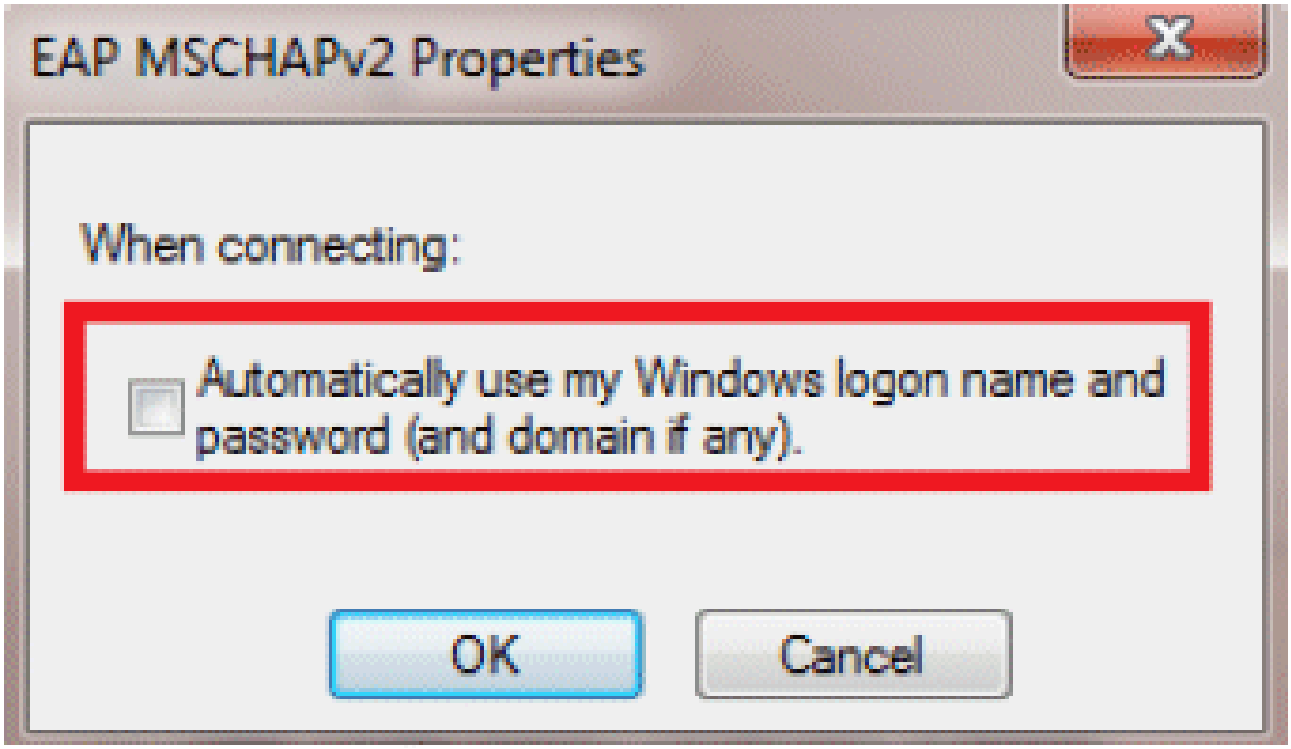

goa Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel



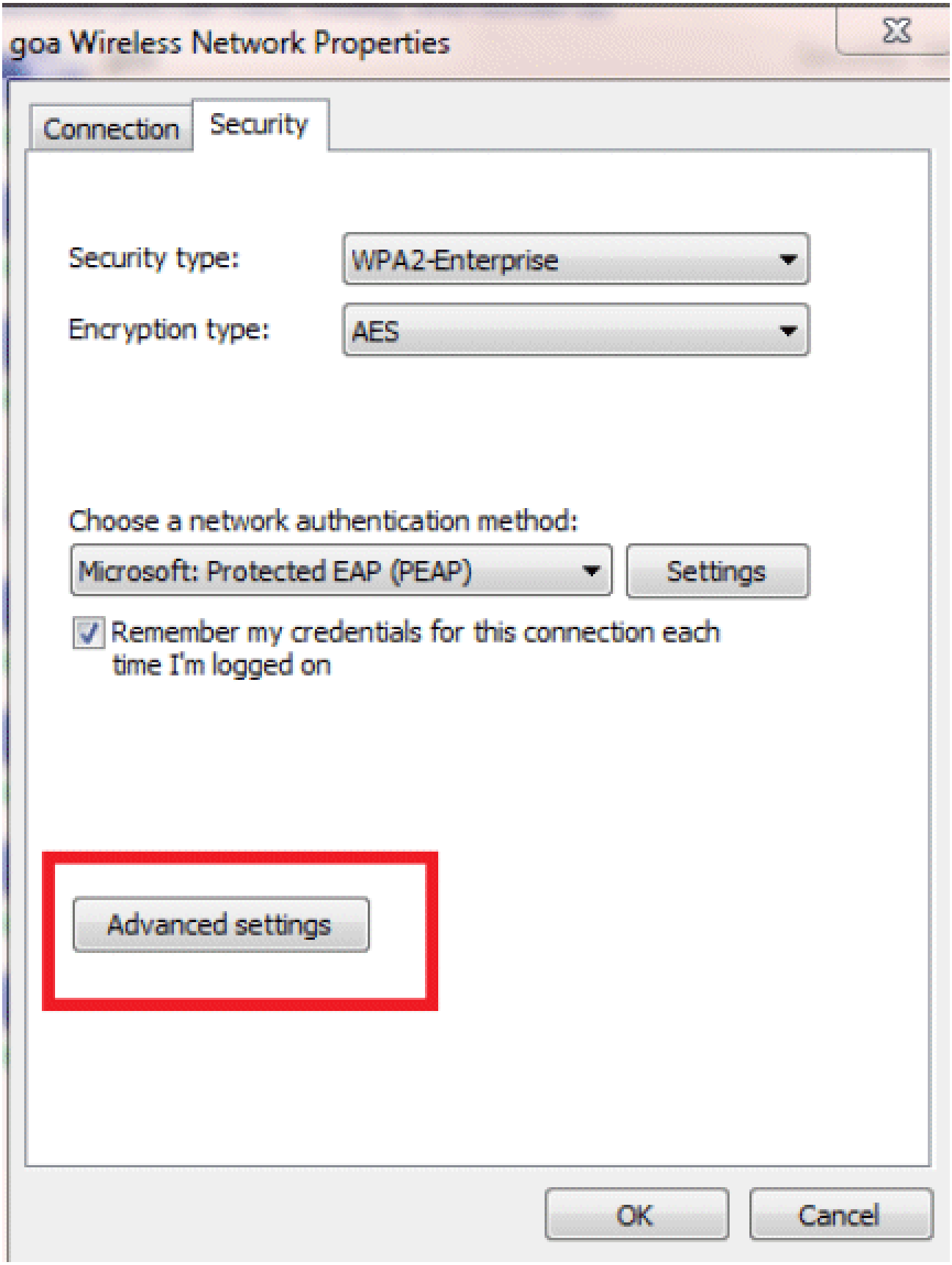
8. 在本示例中，我们未验证服务器证书。如果选中此框且无法连接，请尝试禁用该功能并再次测试。

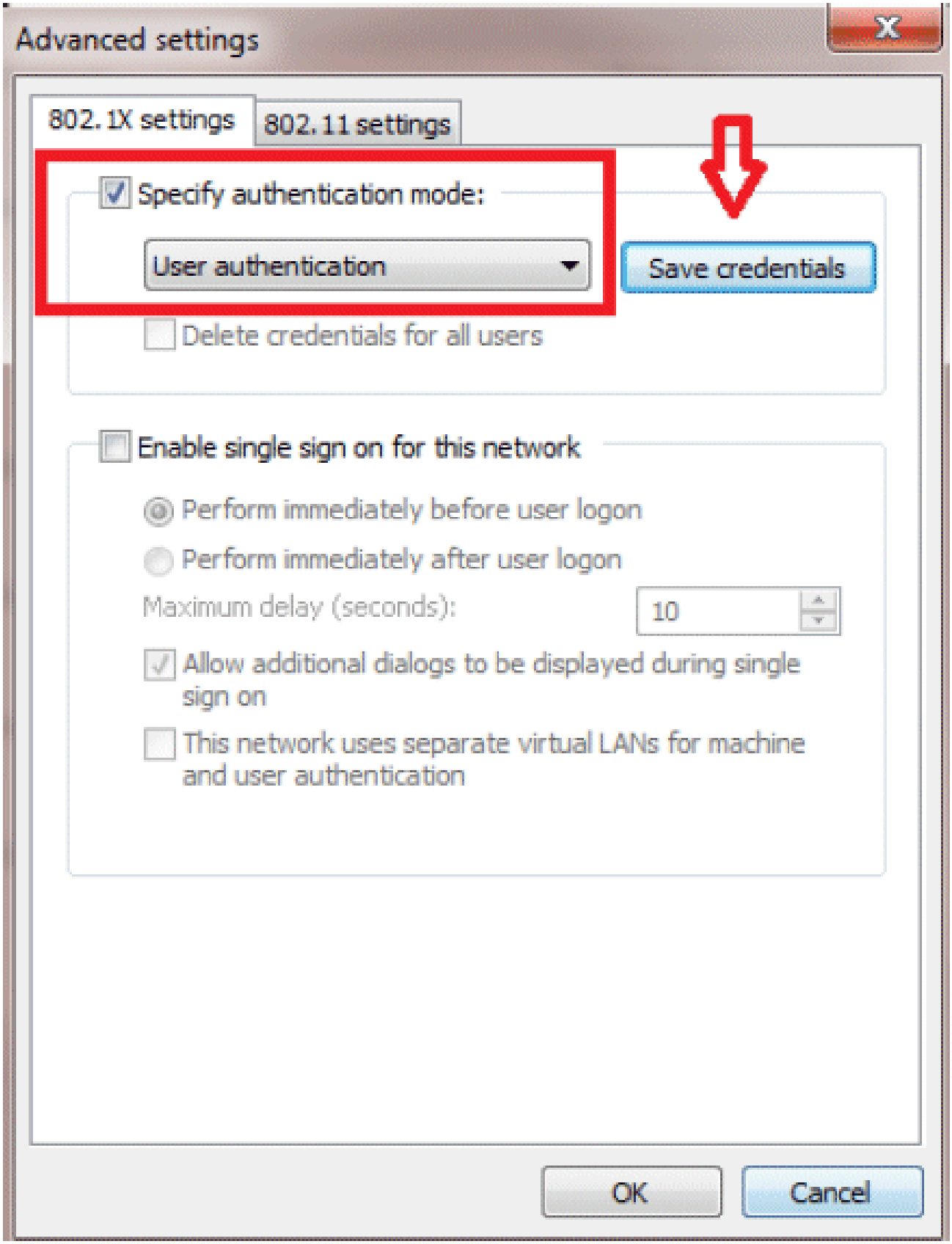


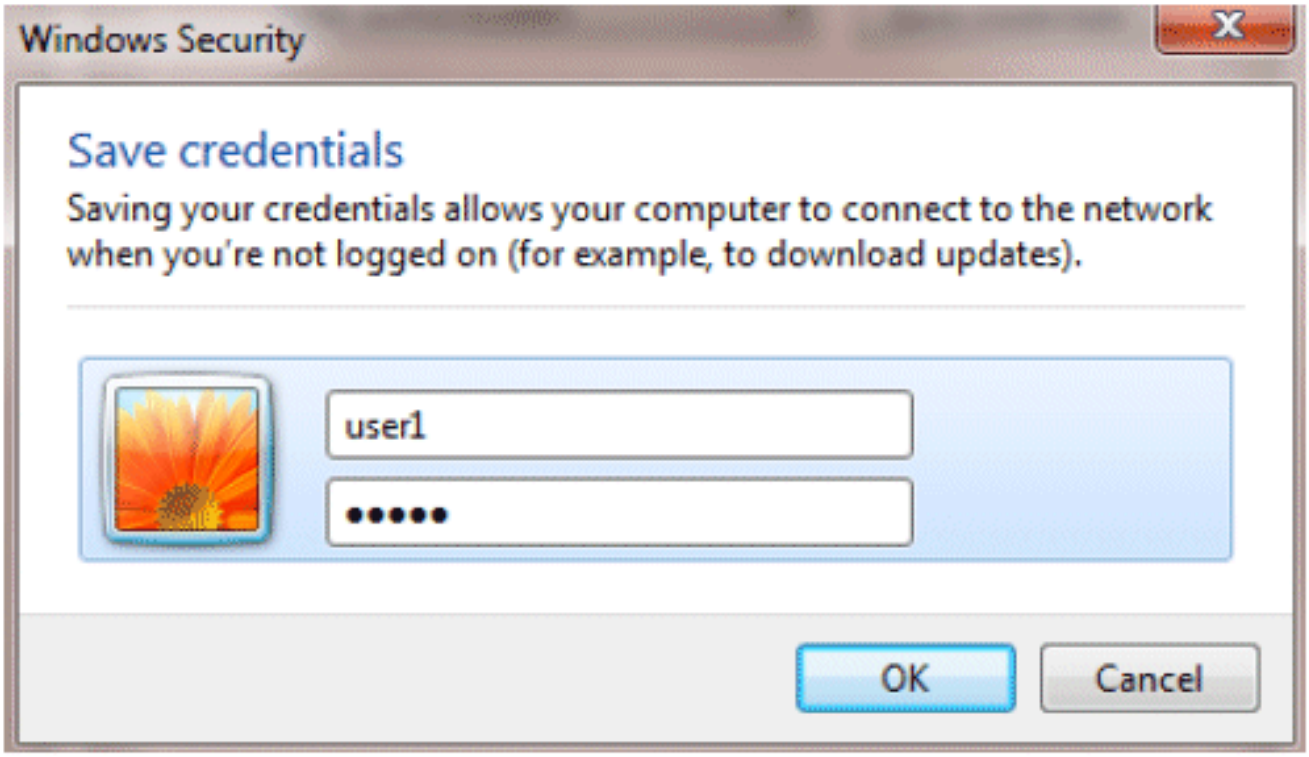
9. 或者，您可以使用您的Windows凭据登录。但是，在本例中，我们不打算使用它。Click OK.



10. 单击Advanced settings以配置用户名和密码。


goa Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel


Advanced settings
802.1X settings
802.11 settings
Specify authentication mode:
User authentication
Save credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds):
10
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK
Cancel



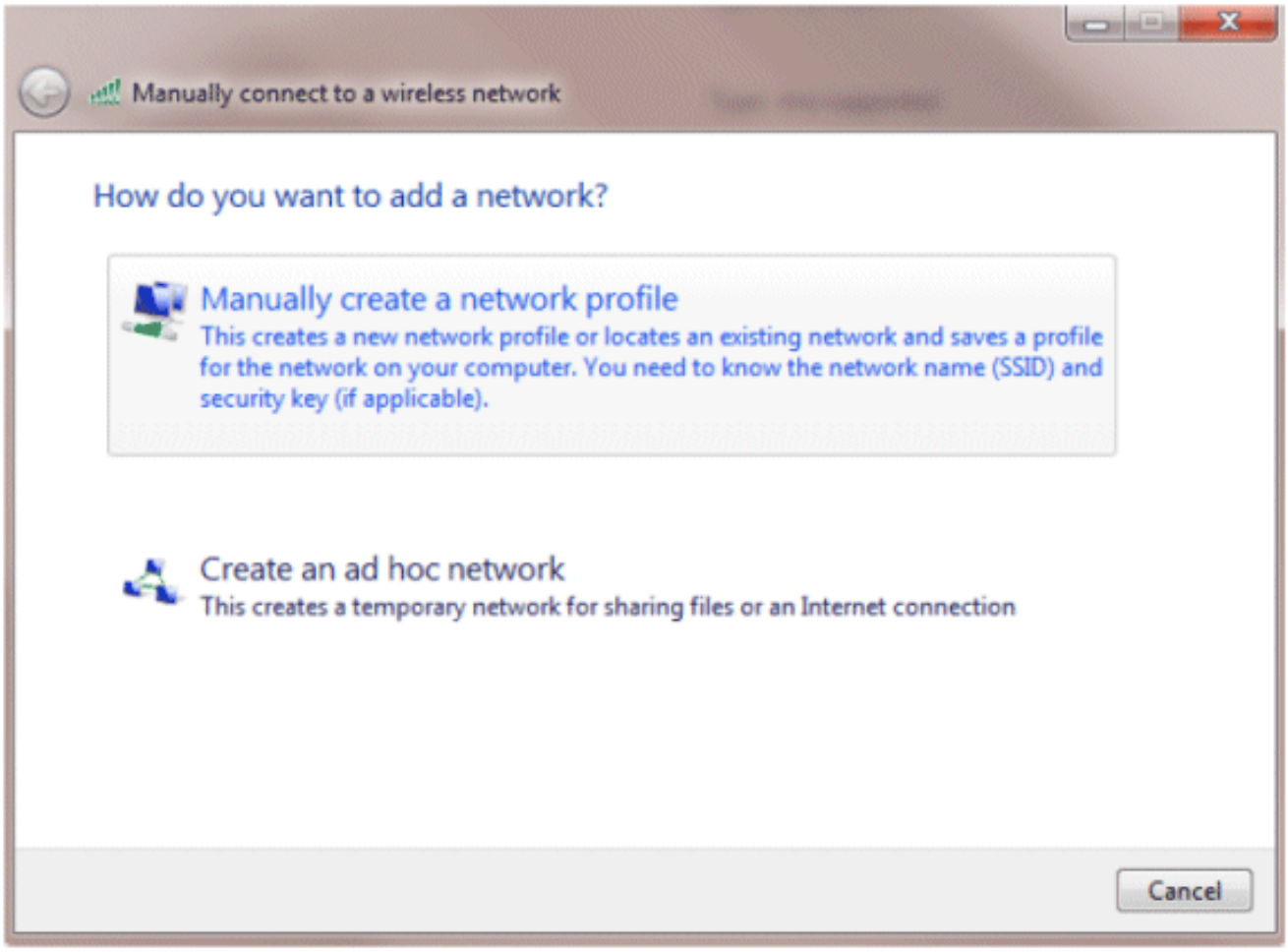
您的客户端实用程序现已准备好连接。

EAP-FAST(user2)

在我们的测试客户端中，我们使用的是运行14.3驱动程序版本的Intel 6300-N卡的Windows 7原生Supplicant客户端。建议使用供应商提供的最新驱动程序进行测试。

要在WZC中创建配置文件，请完成以下步骤：

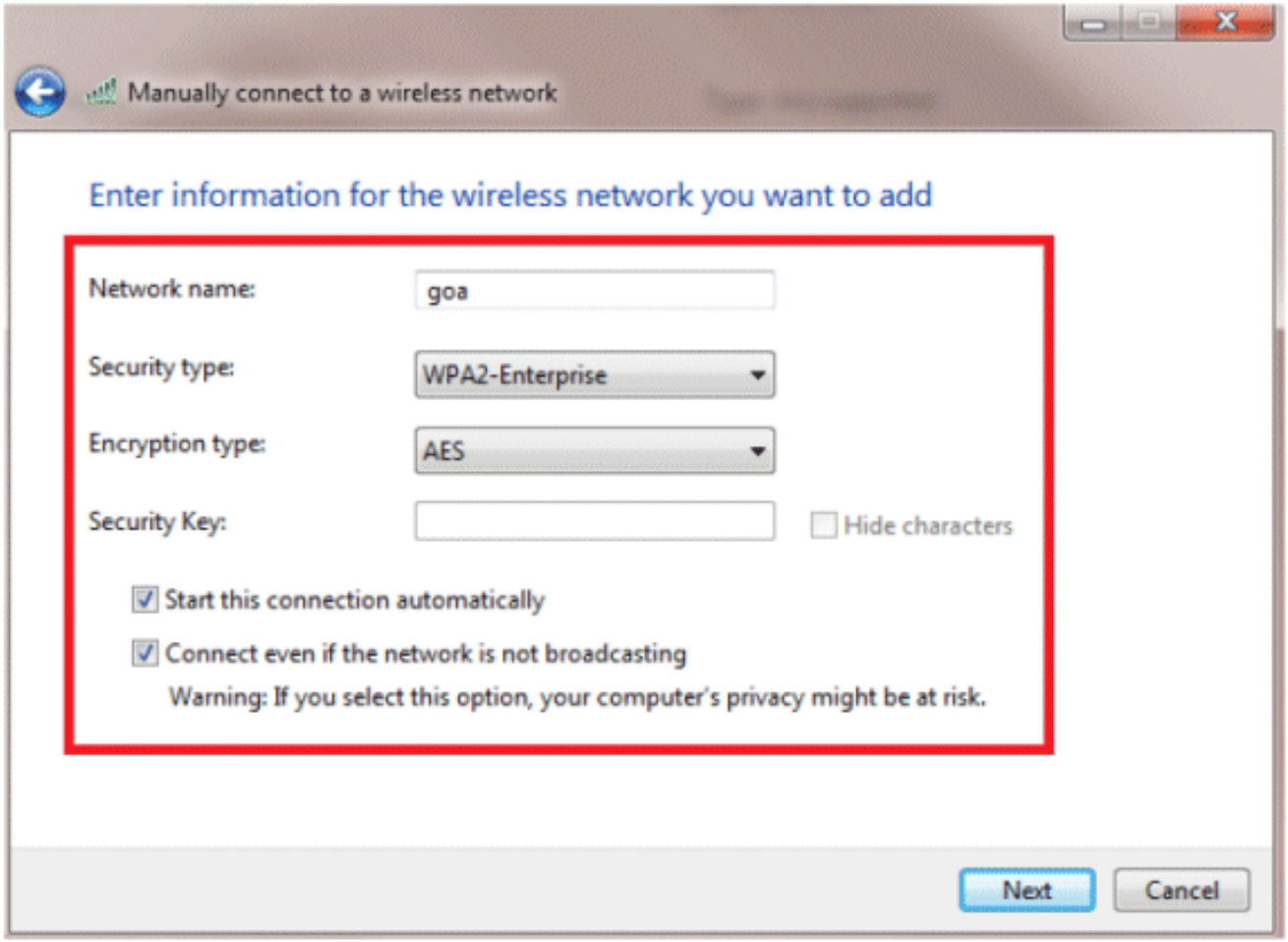
1. 转至控制面板 > 网络和Internet > 管理无线网络。
2. 单击Add选项卡。
3. 单击Manually create a network profile。



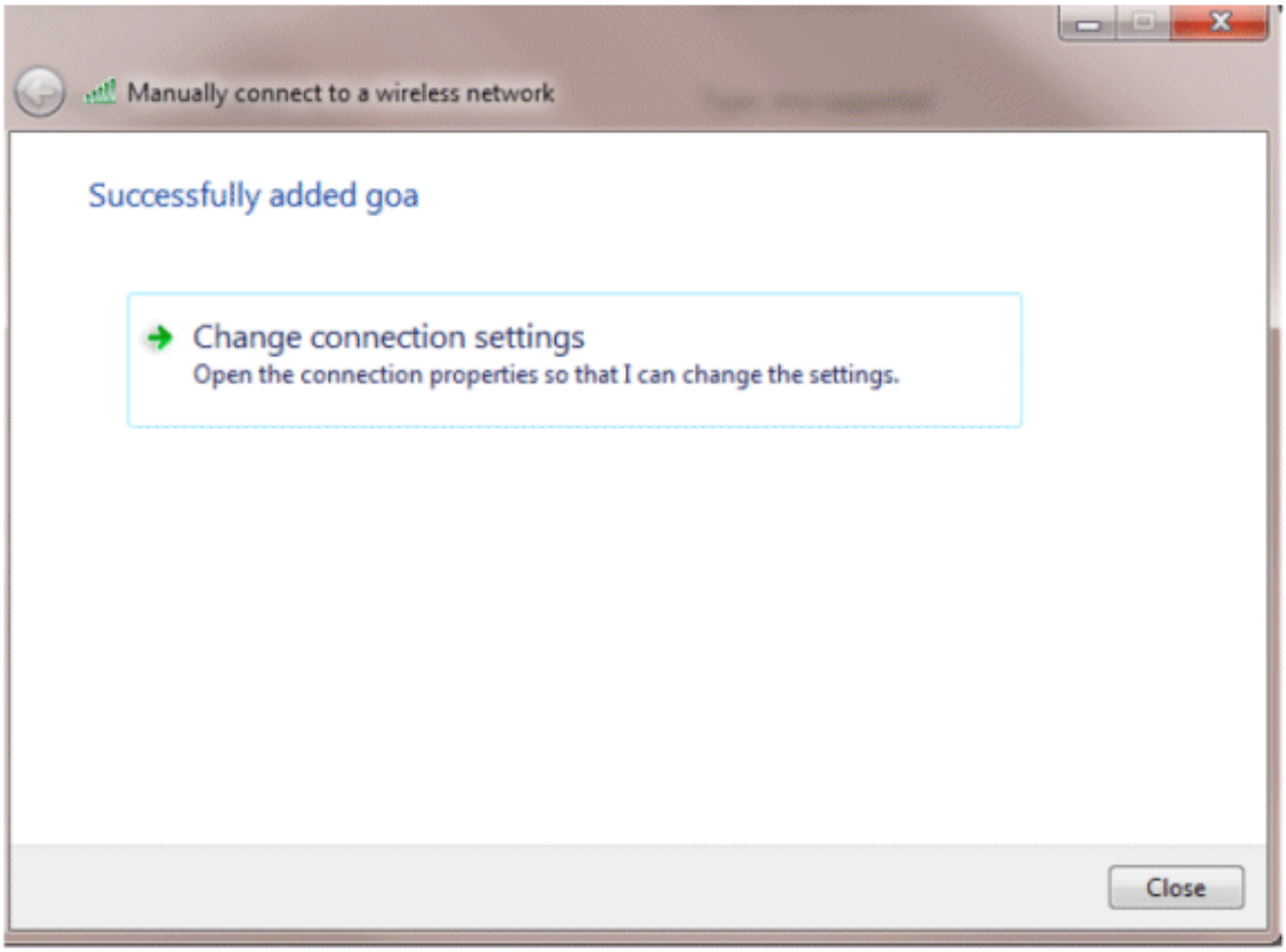
4. 添加在WLC上配置的详细信息。

   注意：SSID区分大小写。

5. 单击 Next。

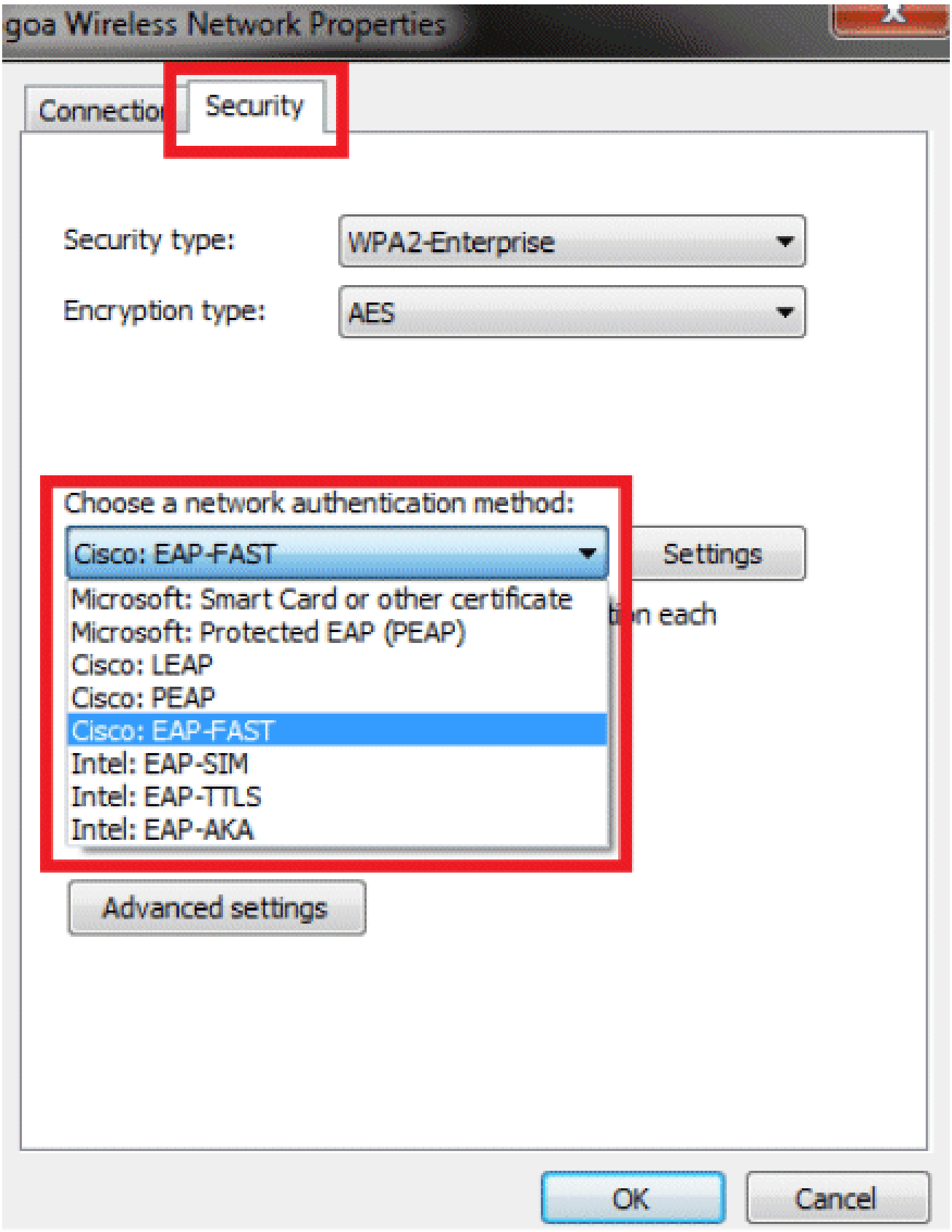


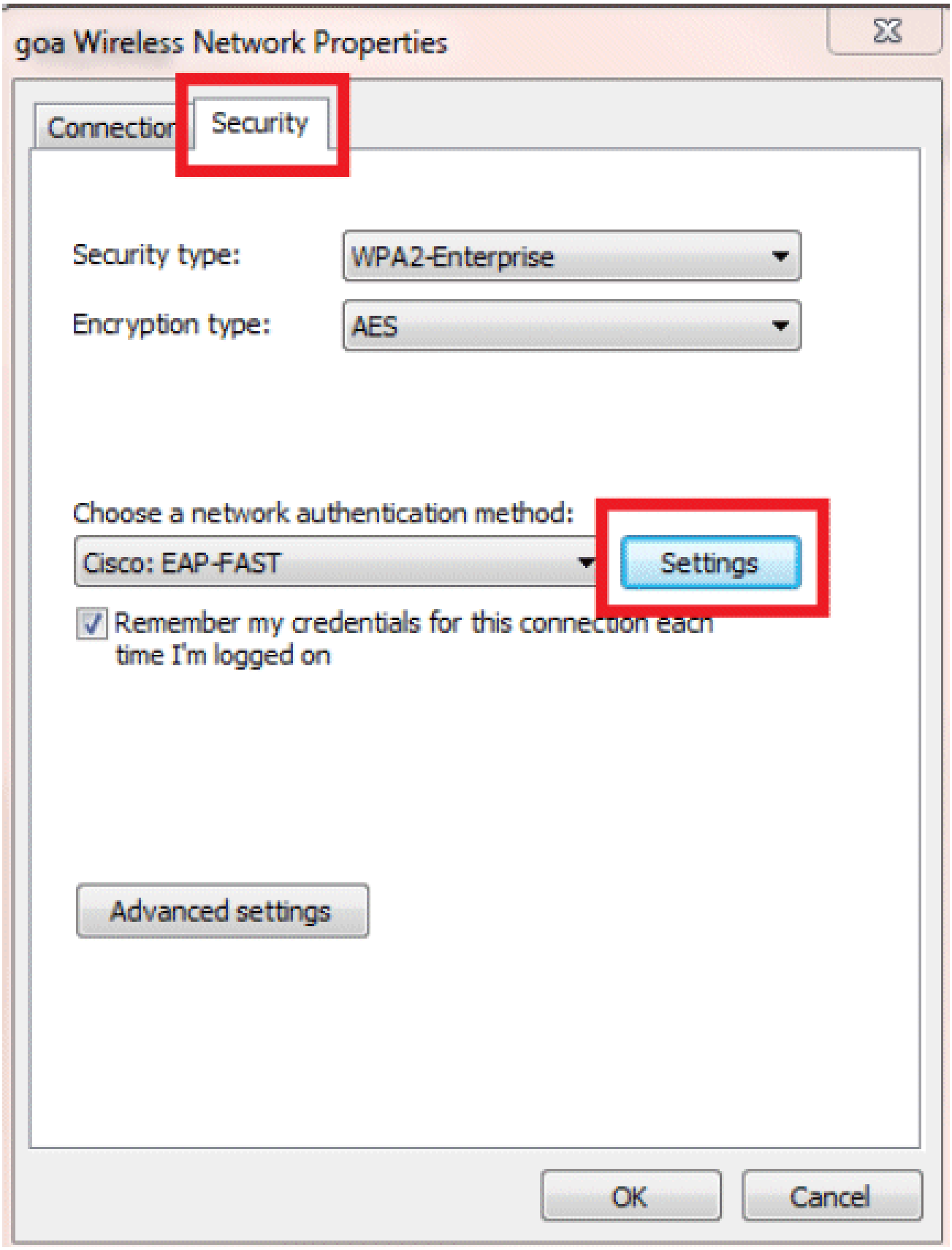
6. 单击Change connection settings以仔细检查设置。



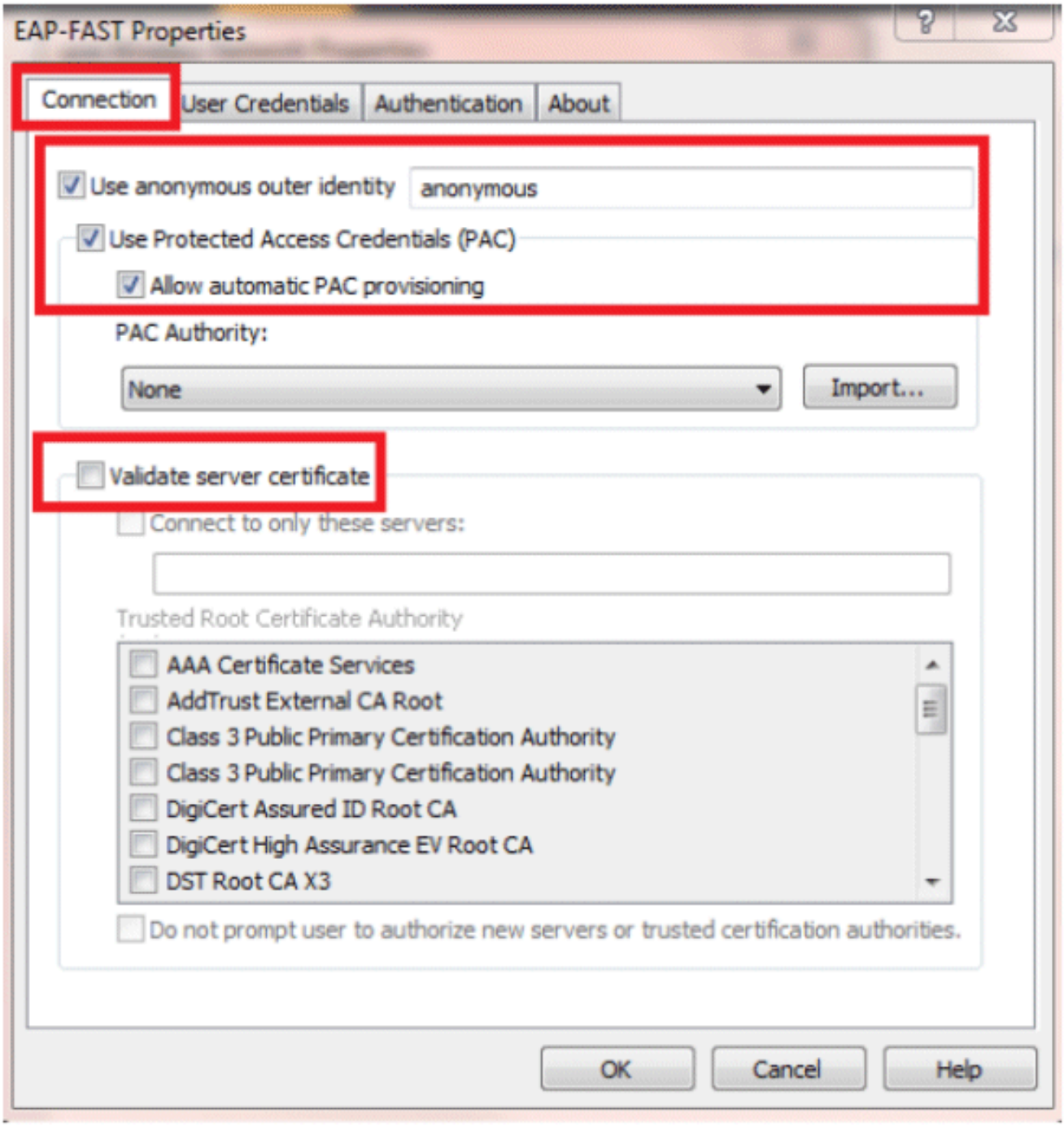
7. 确保已启用EAP-FAST。

注意：默认情况下，WZC没有EAP-FAST作为身份验证方法。您必须从第三方供应商下载该实用程序。在本示例中，由于它是英特尔卡，因此系统中安装了英特尔PROSet。

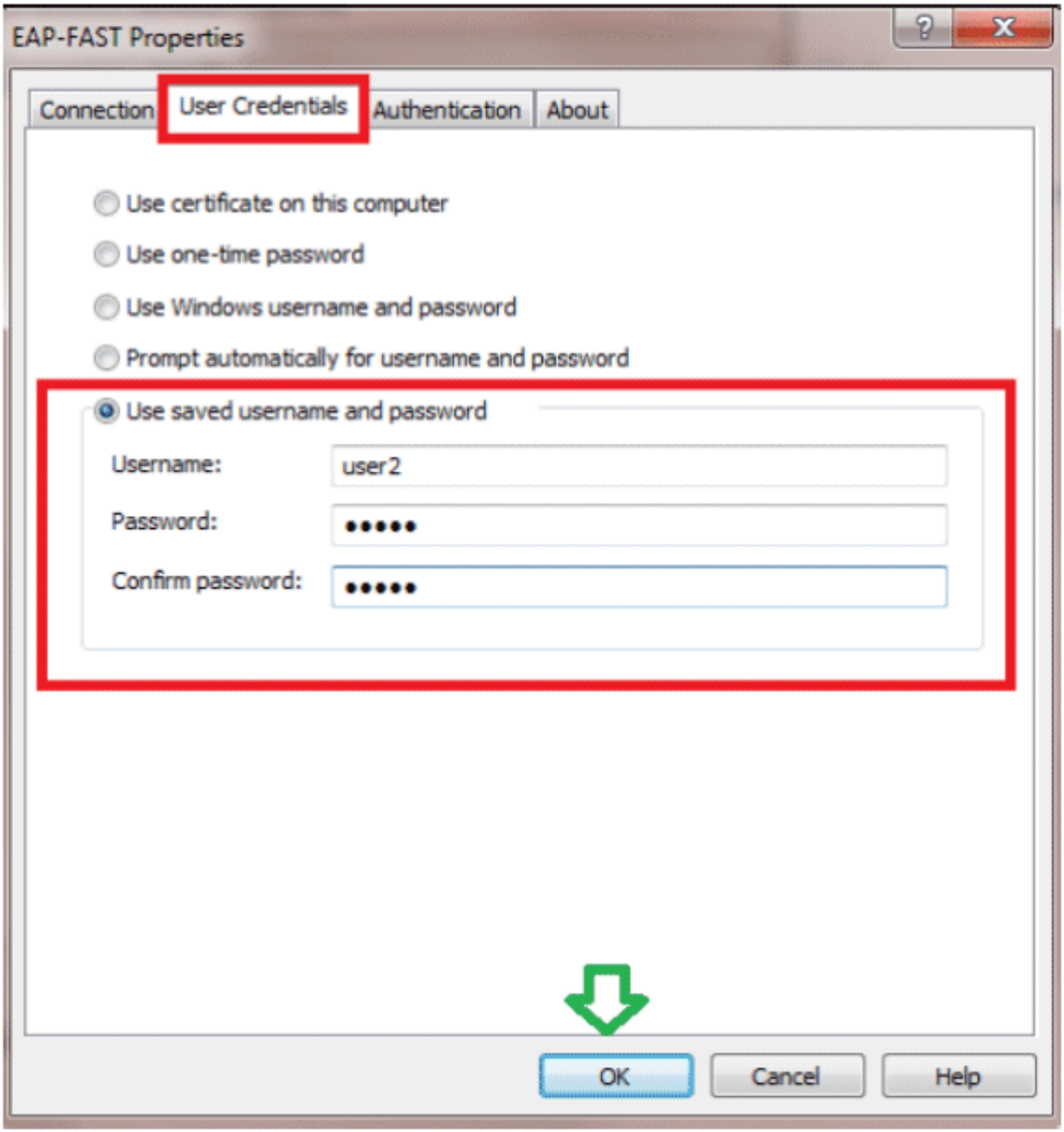

goa Wireless Network Properties
Connectio
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Cisco: EAP-FAST
Settings
Microsoft: Smart Card or other certificate
Microsoft: Protected EAP (PEAP)
Cisco: LEAP
Cisco: PEAP
Cisco: EAP-FAST
Intel: EAP-SIM
Intel: EAP-TTLS
Intel: EAP-AKA
Advanced settings
OK
Cancel



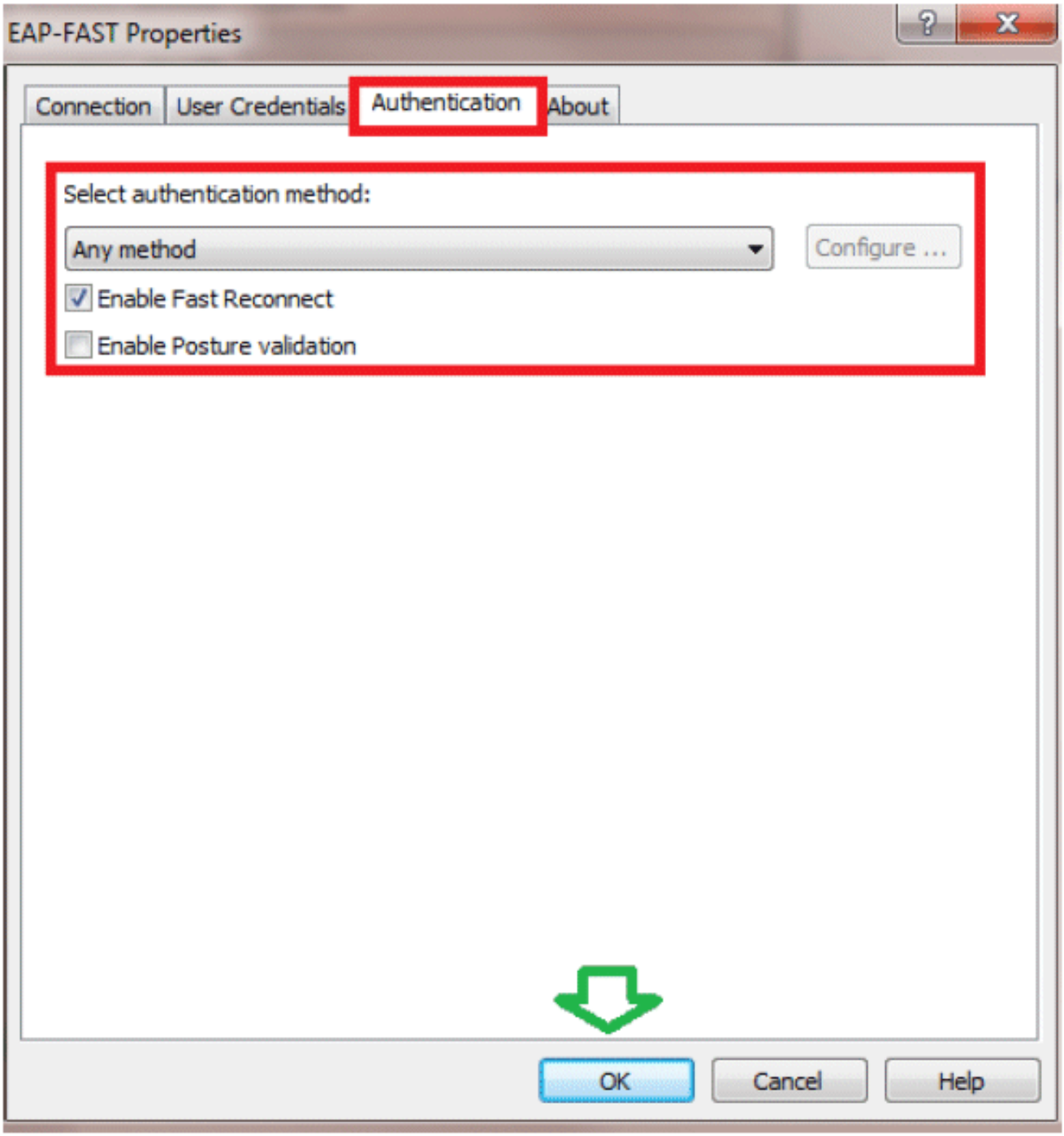
8. 启用Allow automatic PAC provisioning，并确保未选中Validate server certificate。



9. 单击User Credentials选项卡，并输入user2的凭据。或者，您可以使用您的Windows凭据登录。但是，在本例中，我们不打算使用它。

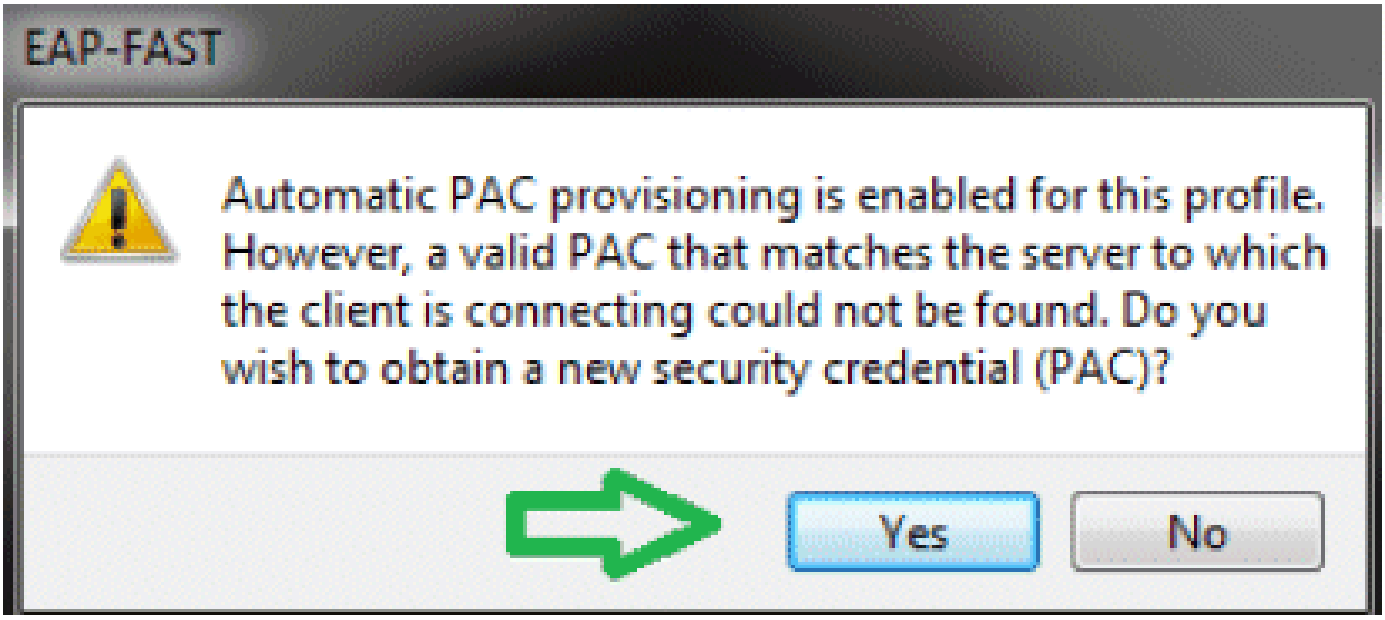

EAP-FAST Properties
Connection
User Credentials
Authentication
About
Use certificate on this computer
Use one-time password
Use Windows username and password
Prompt automatically for username and password
Use saved username and password
Username:
user2
Password:
Confirm password:
OK
Cancel
Help

10. Click OK.



您的客户端实用程序现已准备好连接user2。

注意：当用户2尝试进行身份验证时，RADIUS服务器将发送PAC。接受PAC以完成身份验证。



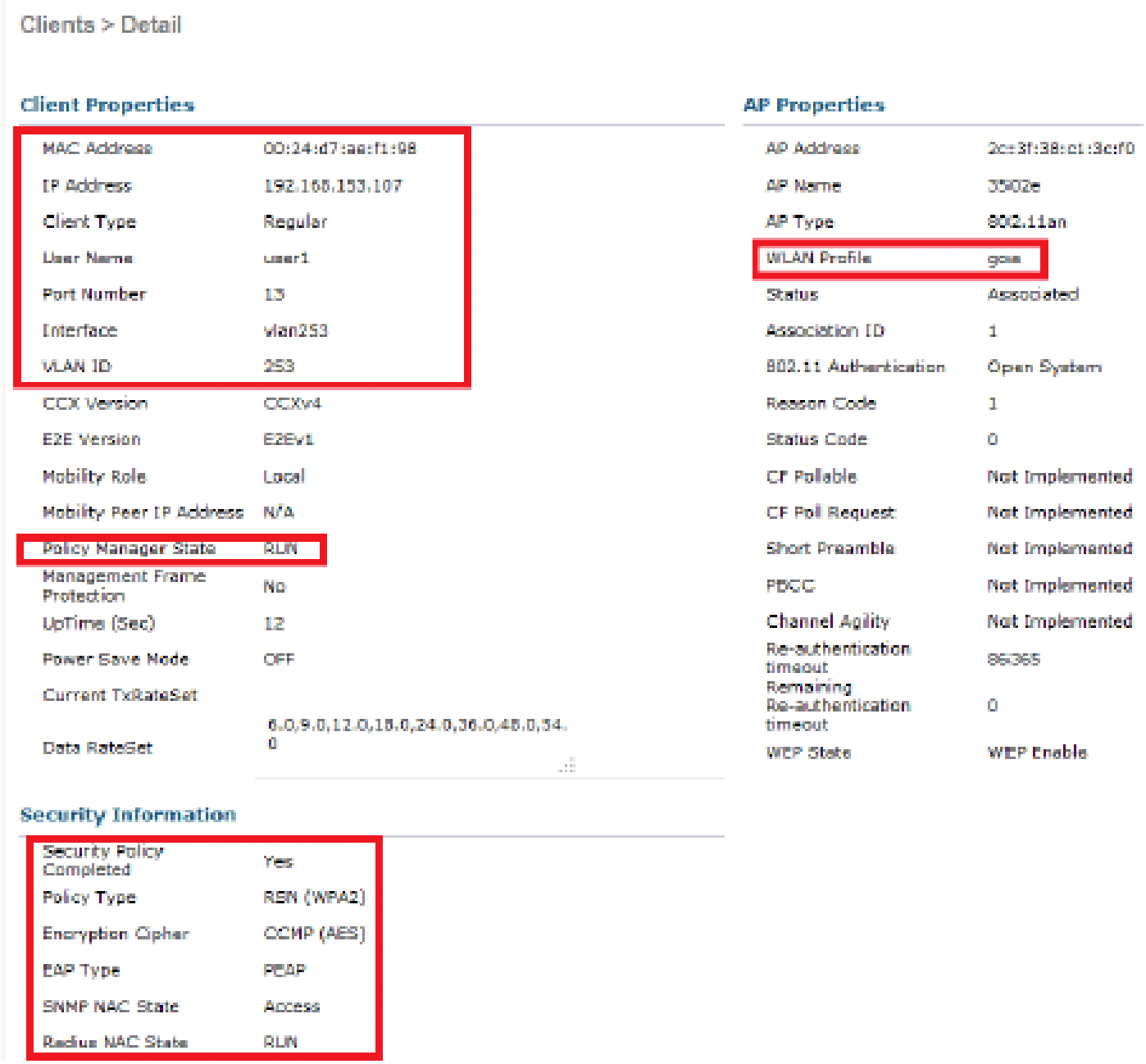
验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

验证user1(PEAP-MSCHAPv2)

从WLC GUI中，转到Monitor > Clients，然后选择MAC地址。



WLC RADIUS统计信息：

<#root>

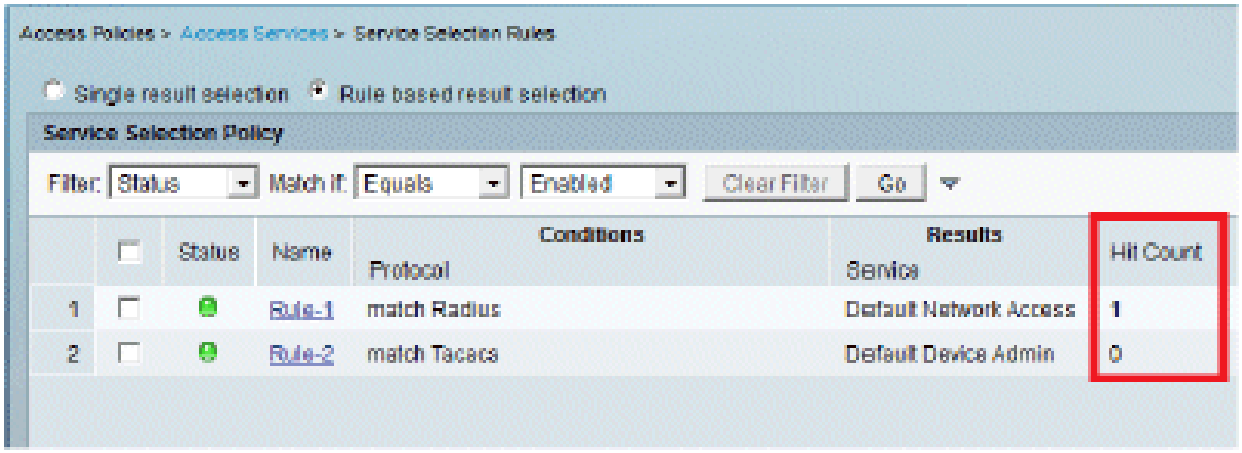
```
(Cisco Controller) >

show radius auth statistics

Authentication Servers:
Server Index..................................... 1
Server Address................................... 192.168.150.24
Msg Round Trip Time.............................. 1 (msec)
First Requests................................... 8
Retry Requests................................... 0
Accept Responses................................. 1
Reject Responses................................. 0
Challenge Responses.............................. 7
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
```

```
Pending Requests.............................. 0
Timeout Requests.............................. 0
Unknowntype Msgs.............................. 0
Other Drops................................... 0
```

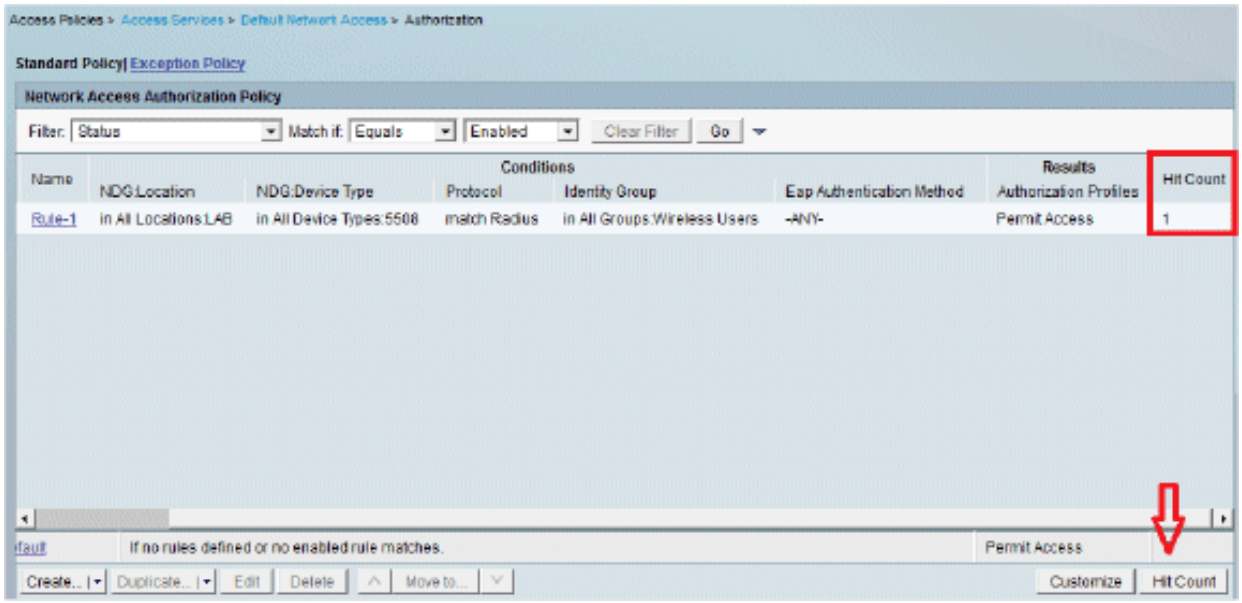
ACS日志：

1. 要查看Hit计数，请完成以下步骤：

   a. 如果在身份验证的15分钟内检查日志，请确保刷新命中计数。



   b. 在同一页底部有一个点击计数选项卡。



2. 单击Monitoring and Reports，此时会显示New弹出窗口。转至Authentications -Radius - Today。您也可以单击Details以验证应用了哪个服务选择规则。

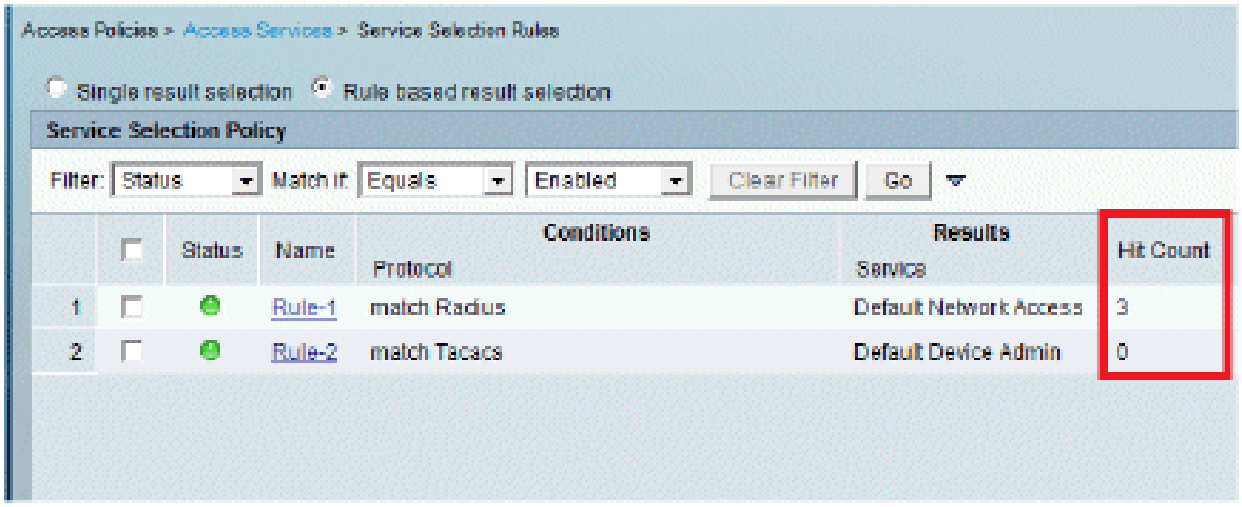
验证user2(EAP-FAST)

从WLC GUI中，转到Monitor > Clients，然后选择MAC地址。

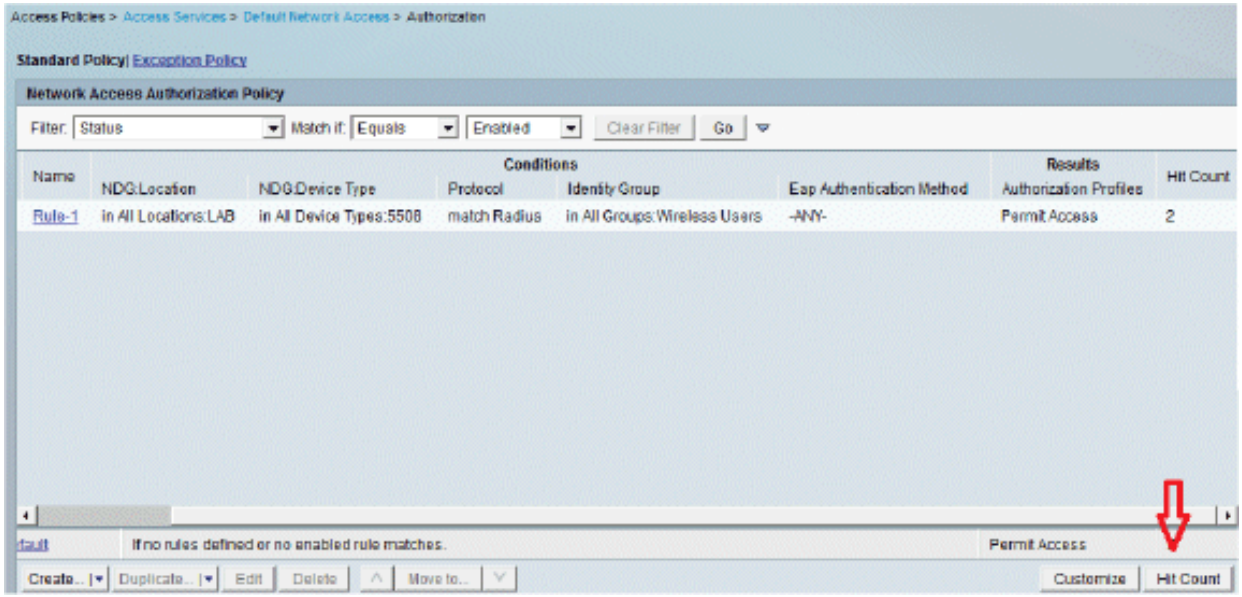
ACS日志：

1. 要查看Hit计数，请完成以下步骤：

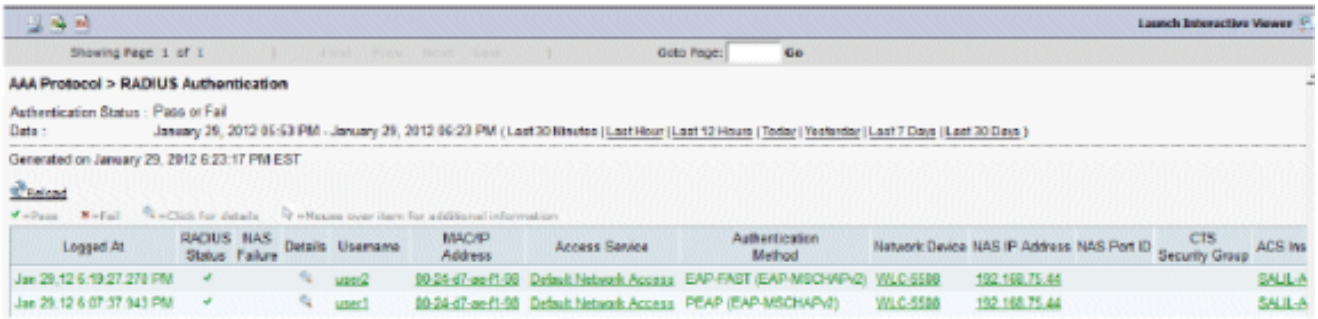
a. 如果在身份验证后15分钟内检查日志，请确保刷新HIT计数。



b. 在同一页底部有一个点击计数选项卡。



2. 单击Monitoring and Reports，此时会显示New弹出窗口。转至Authentications -Radius - Today。您也可以单击Details以验证应用了哪个服务选择规则。



故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

注意：使用debug命令之前，请参阅有关Debug命令的重要信息。

1. 如果遇到任何问题，请在WLC上发出以下命令：
    - debug client <mac add of the client>
    - debug aaa all enable
    - show client detail <mac addr> — 验证策略管理器状态。
    - show radius auth statistics — 验证故障原因。
    - debug disable-all — 关闭调试。
    - clear stats radius auth all - Clear radius statistics on the WLC。
2. 验证ACS中的日志并记录故障原因。

相关信息

- 技术支持和文档 - Cisco Systems

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）。