

# 使用 RADIUS 服务器进行的外部 Web 身份验证

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[网络图](#)

[规则](#)

[外部 Web 身份验证](#)

[配置 WLC](#)

[为 Cisco Secure ACS 配置 WLC](#)

[在 WLC 上配置用于 Web 身份验证的 WLAN](#)

[在 WLC 上配置 Web 服务器信息](#)

[配置 Cisco Secure ACS](#)

[在 Cisco Secure ACS 上配置用户信息](#)

[在 Cisco Secure ACS 上配置 WLC 信息](#)

[客户端身份验证过程](#)

[客户端配置](#)

[客户端登录过程](#)

[验证](#)

[验证 ACS](#)

[验证 WLC](#)

[故障排除](#)

[故障排除命令](#)

[相关信息](#)

## 简介

本文介绍如何使用外部 RADIUS 服务器执行外部 Web 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：

- 了解轻量接入点 (LAP) 和 Cisco WLC 配置的基础知识
- 有关如何设置和配置外部 Web 服务器的知识
- 有关如何配置 Cisco Secure ACS 的知识

## [使用的组件](#)

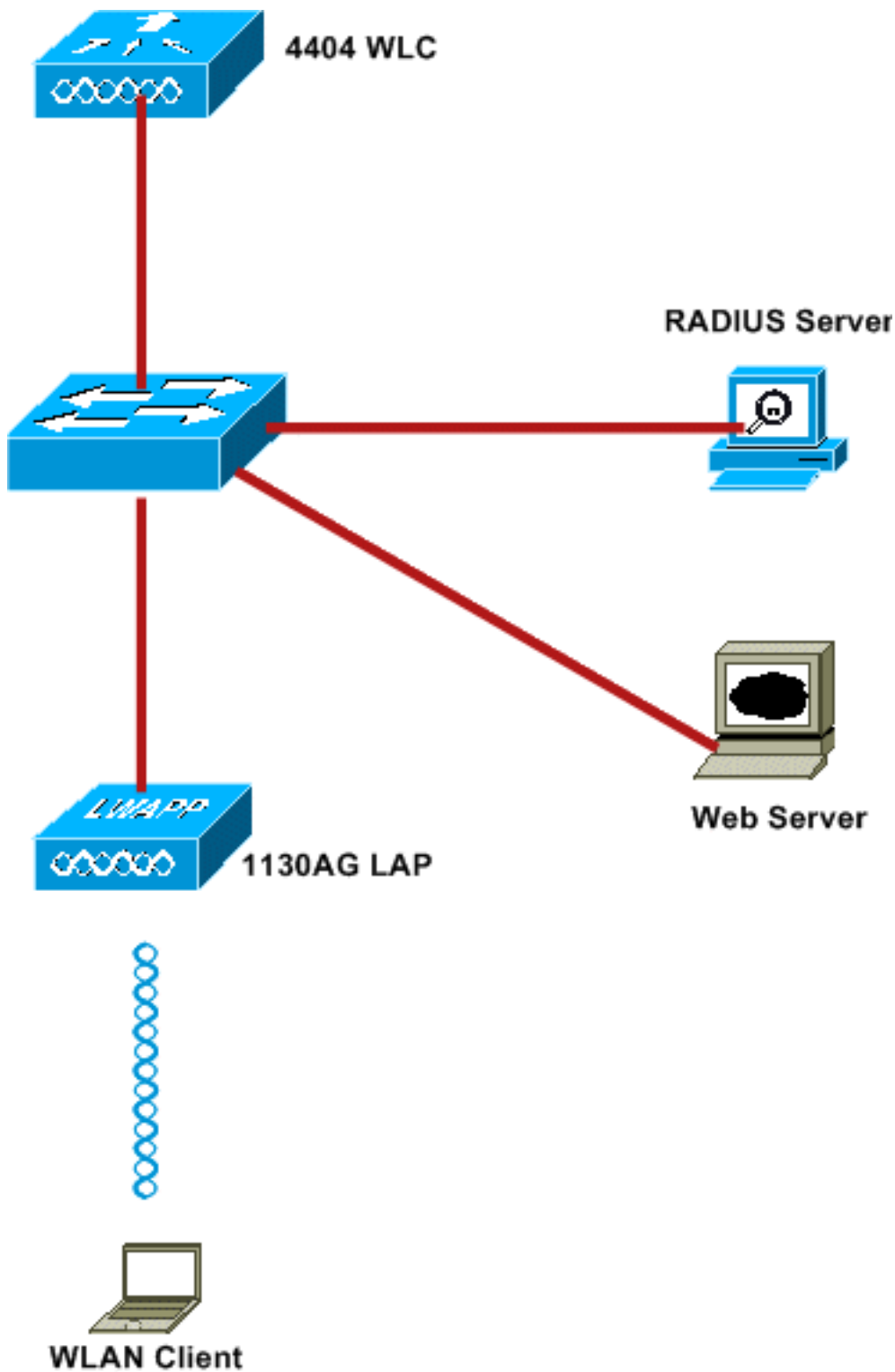
本文档中的信息基于以下软件和硬件版本：

- 运行固件版本 5.0.148.0 的无线 LAN 控制器
- Cisco 1232 系列 LAP
- Cisco 802.11a/b/g 无线客户端适配器 3.6.0.61
- 托管 Web 身份验证登录页面的外部 Web 服务器
- 运行固件版本 4.1.1.24 的 Cisco Secure ACS 版本

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。

## [网络图](#)

本文档使用以下网络设置：



以下是本文档中使用的 IP 地址：

- WLC 使用 IP 地址 10.77.244.206
- LAP 已使用 IP 地址 10.77.244.199 注册到 WLC
- Web 服务器使用 IP 地址 10.77.244.210
- Cisco ACS 服务器使用 IP 地址 10.77.244.196
- 客户端收到来自管理接口的一个映射到 WLAN 的 IP 地址 - 10.77.244.208

## 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## [外部 Web 身份验证](#)

Web 身份验证是第 3 层身份验证机制，用于对来宾用户进行身份验证以进行 Internet 访问。使用此过程进行验证的用户在其成功完成验证过程之前无法访问 Internet。有关外部 Web 身份验证过程的完整信息，请阅读文档[使用无线 LAN 控制器进行外部 Web 身份验证配置的示例](#)的[外部 Web 身份验证过程](#)部分。

在本文中，我们来看看一个配置示例，该示例中使用外部 RADIUS 服务器执行外部 Web 身份验证。

## [配置 WLC](#)

在本文中，我们假设 WLC 已配置且具有一个注册到 WLC 的 LAP。此外，本文档进一步假设已配置 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 \(LAP\)](#)。要查看注册到 WLC 的 LAP，请导航到 **Wireless > All APs**。

一旦配置 WLC 进行基本操作并在其中注册一个或多个 LAP，即可使用外部 Web 服务器为外部 Web 身份验证配置 WLC。在本示例中，我们使用 Cisco Secure ACS 4.1.1.24 版作为 RADIUS 服务器。首先，我们将配置此 RADIUS 服务器的 WLC，然后我们将查看 Cisco Secure ACS 上关于此设置所需的配置。

## [为 Cisco Secure ACS 配置 WLC](#)

执行这些步骤以便在 WLC 上添加 RADIUS 服务器：

1. 从 WLC GUI 中，单击 **Security** 菜单。
2. 在 **AAA** 菜单下，导航到 **Radius > Authentication** 子菜单。
3. 单击 **New**，并输入 RADIUS 服务器的 IP 地址。在本示例中，服务器的 IP 地址为 **10.77.244.196**。
4. 在 WLC 中输入共享密钥。共享密钥在 WLC 上的配置应相同。
5. 选择 **ASCII** 或 **Hex** 为共享密钥格式。在 WLC 上需要选择同一格式。
6. **1812** 是用于 RADIUS 验证的端口号。
7. 确保 **Server Status** 选项设置为 **Enabled**。
8. 选中 **Network User Enable** 框以对网络用户进行身份验证。
9. 单击 **适用**。

The screenshot shows the Cisco WLC GUI for configuring a new RADIUS Authentication Server. The left sidebar is under 'Security' with 'AAA' expanded to 'RADIUS'. The main area is titled 'RADIUS Authentication Servers > New' and contains the following configuration fields:

- Server Index (Priority): 2
- Server IP Address: 10.77.244.196
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Key Wrap:  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled
- Support for RFC 3576: Enabled
- Server Timeout: 2 seconds
- Network User:  Enable
- Management:  Enable
- IPSec:  Enable

## [在 WLC 上配置用于 Web 身份验证的 WLAN](#)

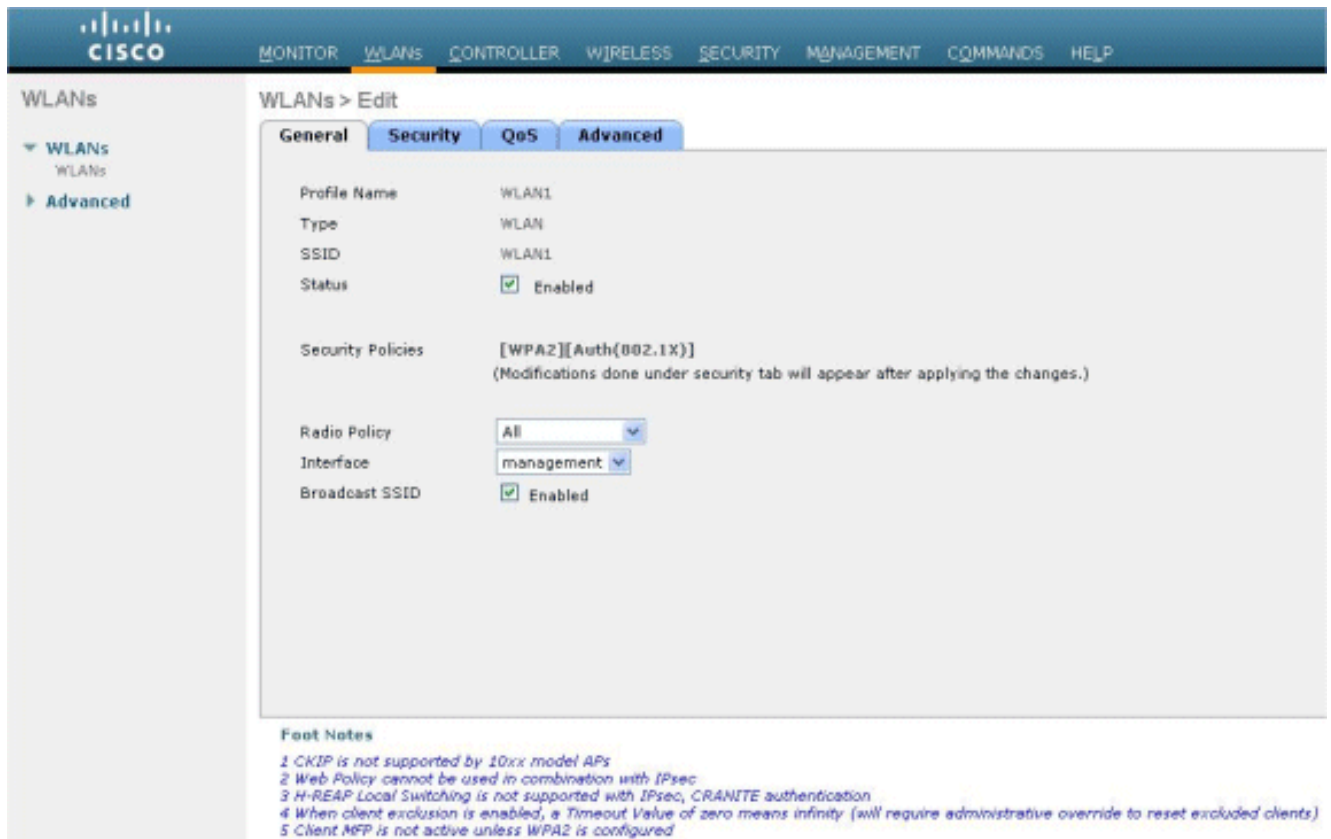
下一步是在 WLC 上为 Web 身份验证配置 WLAN。执行这些步骤以便在 WLC 上配置 WLAN：

1. 从控制器 GUI 中单击 **WLAN** 菜单，并选择 **New**。
2. 选择 **WLAN** 作为类型。
3. 输入配置文件名称和您所选的 WLAN SSID，并单击 **Apply**。注意：WLAN SSID 区分大小写。

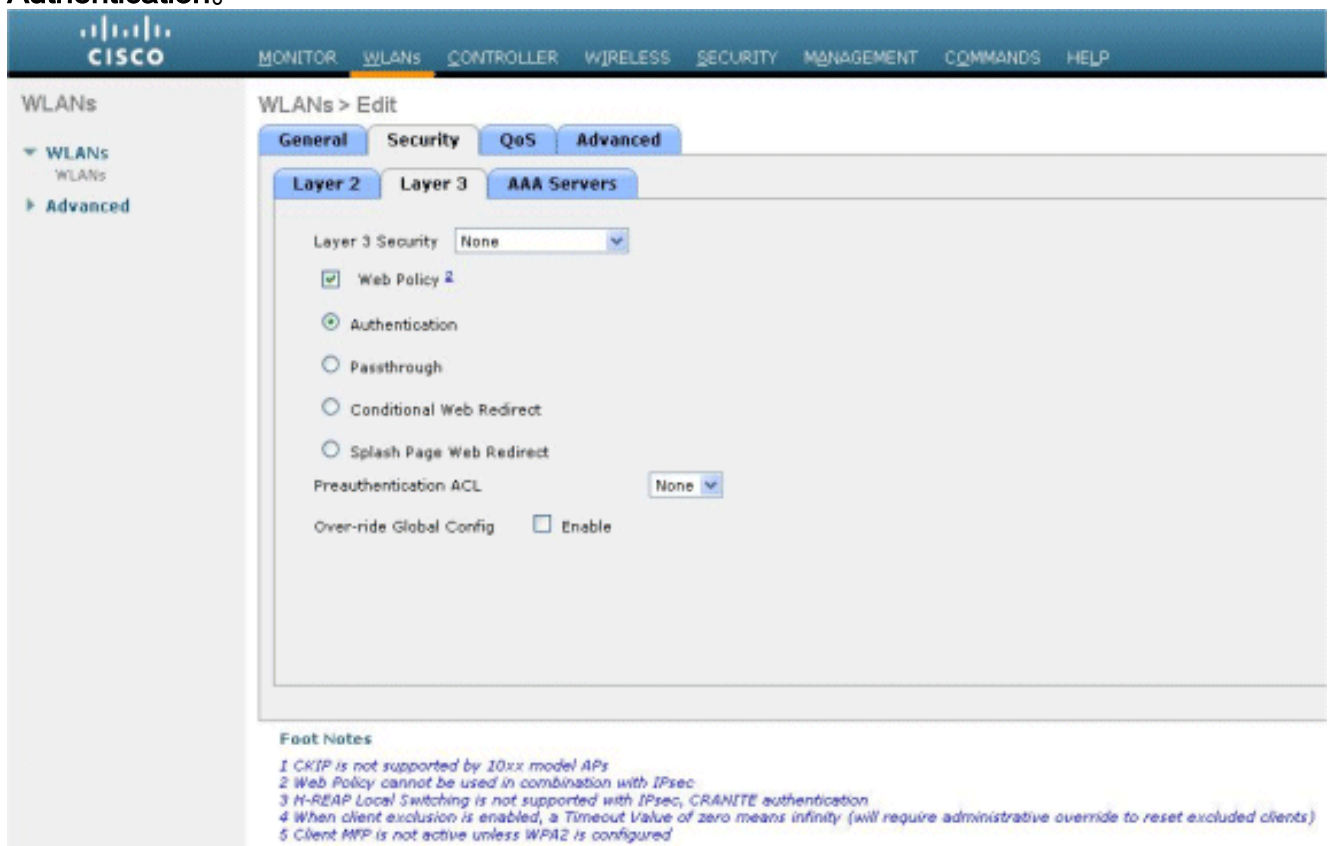
The screenshot shows the Cisco WLC GUI for configuring a new WLAN. The left sidebar is under 'WLANs' with 'Advanced' expanded. The main area is titled 'WLANs > New' and contains the following configuration fields:

- Type: WLAN
- Profile Name: WLAN1
- WLAN SSID: WLAN1

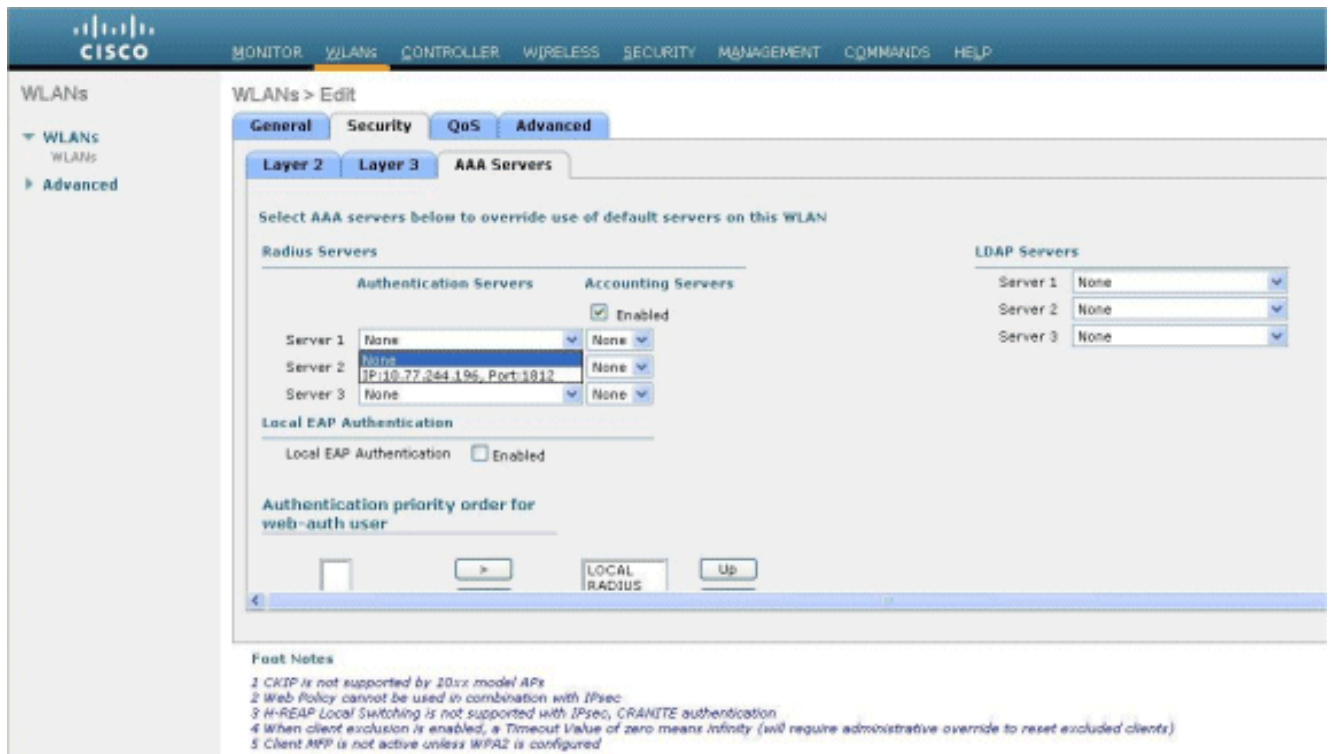
4. 在 **General** 选项卡下，确保为 Status 和 Broadcast SSID 选中了 **Enabled** 选项。**WLAN配置**



5. 为 WLAN 选择一个接口。通常，唯一 VLAN 中配置的接口将映射到 WLAN，以便客户端能接收该 VLAN 中的一个 IP 地址。在本例中，我们使用管理接口。
6. 选择 **Security** 选项卡。
7. 在 **Layer 2** 菜单下，为 Layer 2 Security 选择 **None**。
8. 在 **Layer 3** 菜单下，为 Layer 3 Security 选择 **None**。选中 **Web Policy** 复选框并选择 **Authentication**。



9. 在 **AAA servers** 菜单下，对于身份验证服务器，请选择在此 WLC 上配置的 RADIUS 服务器。其他菜单应保留默认值。

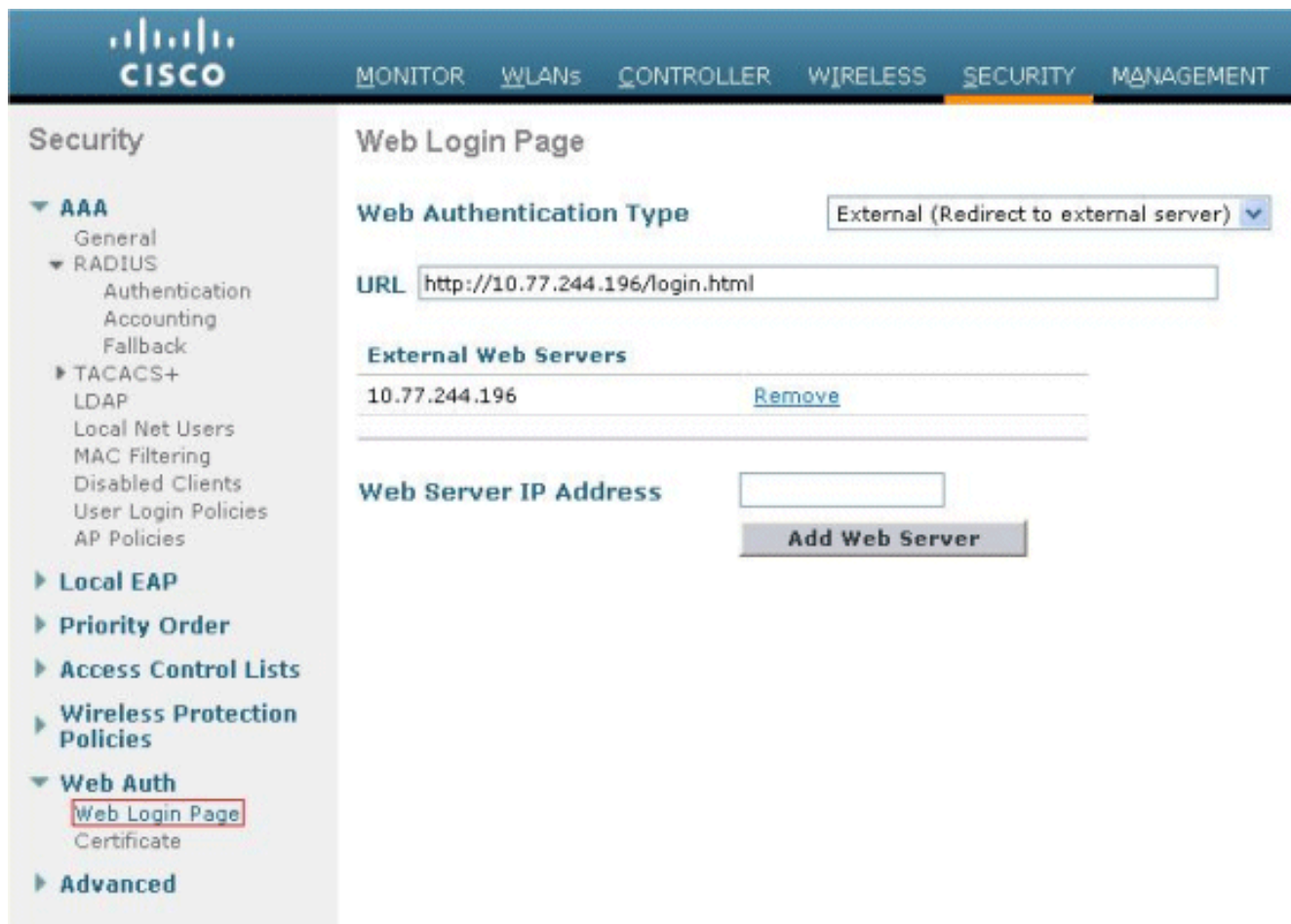


## 在 WLC 上配置 Web 服务器信息

托管 Web 验证页的 Web 服务器应在 WLC 上进行配置。执行这些步骤以配置 Web 服务器：

1. 点击安全选项。转到 **Web Auth > Web Login Page**。
2. 将 Web 身份验证类型设置为 **External**。
3. 在 Web Server IP Address 字段中，输入托管 Web 身份验证页的服务器的 IP 地址，并单击 **Add Web Server**。在本例中，IP 地址是 `10.77.244.196`，显示在外部 Web 服务器下。
4. 在 URL 字段中输入 Web 身份验证页的 URL（在本例中为 `http://10.77.244.196/login.html`）。





## 配置 Cisco Secure ACS

在本文中，我们假设 Cisco Secure ACS 服务器已安装并在计算机上运行。有关如何设置 Cisco Secure ACS 的详细信息，请参阅 [Cisco Secure ACS 4.2 配置指南](#)。

### [在 Cisco Secure ACS 上配置用户信息](#)

执行这些步骤以便在 Cisco Secure ACS 上配置用户：

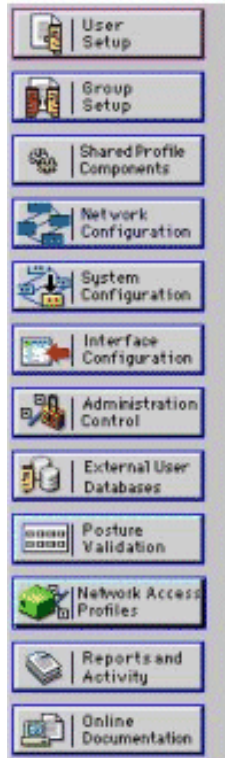
1. 从 Cisco Secure ACS GUI 中选择 **User Setup**，输入用户名，并单击 **Add/Edit**。在本例中，用户为 *user1*。





## User Setup

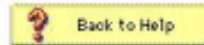
Select



User:

List users beginning with letter/number:

<a href="#">A</a>	<a href="#">B</a>	<a href="#">C</a>	<a href="#">D</a>	<a href="#">E</a>	<a href="#">F</a>	<a href="#">G</a>	<a href="#">H</a>	<a href="#">I</a>	<a href="#">J</a>	<a href="#">K</a>	<a href="#">L</a>	<a href="#">M</a>
<a href="#">N</a>	<a href="#">O</a>	<a href="#">P</a>	<a href="#">Q</a>	<a href="#">R</a>	<a href="#">S</a>	<a href="#">T</a>	<a href="#">U</a>	<a href="#">V</a>	<a href="#">W</a>	<a href="#">X</a>	<a href="#">Y</a>	<a href="#">Z</a>
<a href="#">0</a>	<a href="#">1</a>	<a href="#">2</a>	<a href="#">3</a>	<a href="#">4</a>	<a href="#">5</a>	<a href="#">6</a>	<a href="#">7</a>	<a href="#">8</a>	<a href="#">9</a>			



- 默认情况下，PAP 用于验证客户端。用户的密码在 **User Setup > Password Authentication > Cisco Secure PAP** 下输入。确保您选择 **ACS Internal Database** 进行密码验证。



## User Setup

Edit

### User: user1 (New User)

Account Disabled

#### Supplementary User Info

Real Name:

Description:

---

#### User Setup

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password:

Confirm Password:

Separate (CHAP/MS-CHAP/ARAP)

Password:

Confirm Password:

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

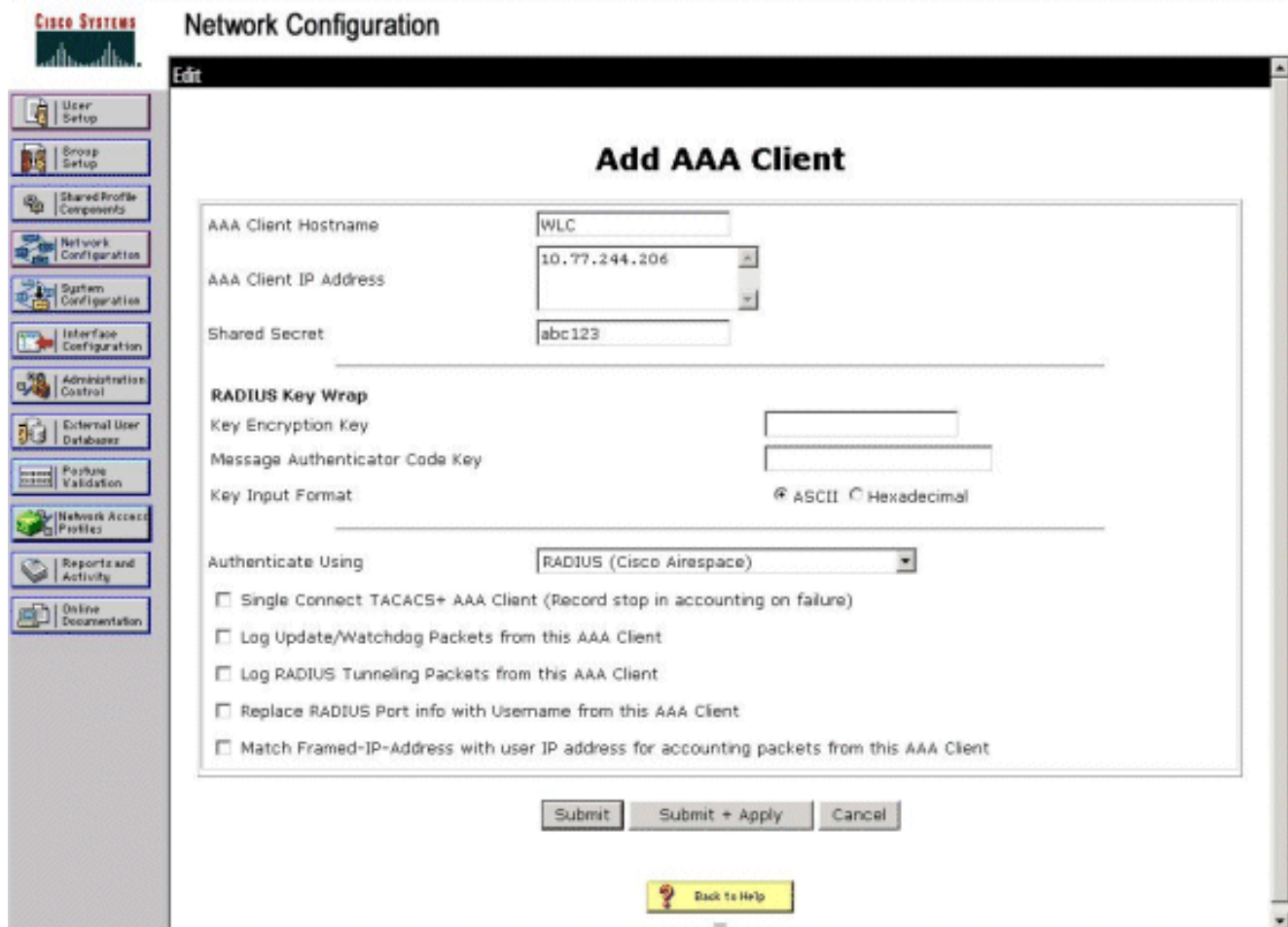
Group to which the user is assigned:

3. 需要向用户分配用户所属的组。选择 **Default Group**。
4. 点击**提交**。

## [在 Cisco Secure ACS 上配置 WLC 信息](#)

执行这些步骤以便在 Cisco Secure ACS 上配置 WLC 信息：

1. 在 ACS GUI 中，单击 **Network Configuration** 选项卡，并单击 **Add Entry**。
2. Add AAA client 屏幕将显示。
3. 输入客户端的名称。在本例中，我们使用 **WLC**。
4. 输入客户端的 IP 地址。WLC 的 IP 地址是 **10.77.244.206**。
5. 输入共享密钥和密钥格式。这应该与 WLC 的 **Security** 菜单中设置的条目相匹配。
6. 选择 **ASCII** 作为关键词输入格式，这在 WLC 上应该是相同的。
7. 选择 **RADIUS (Cisco Airespace)** 用于进行身份验证，以便设置 WLC 和 RADIUS 服务器之间使用的协议。
8. 单击 **Submit+Apply**。



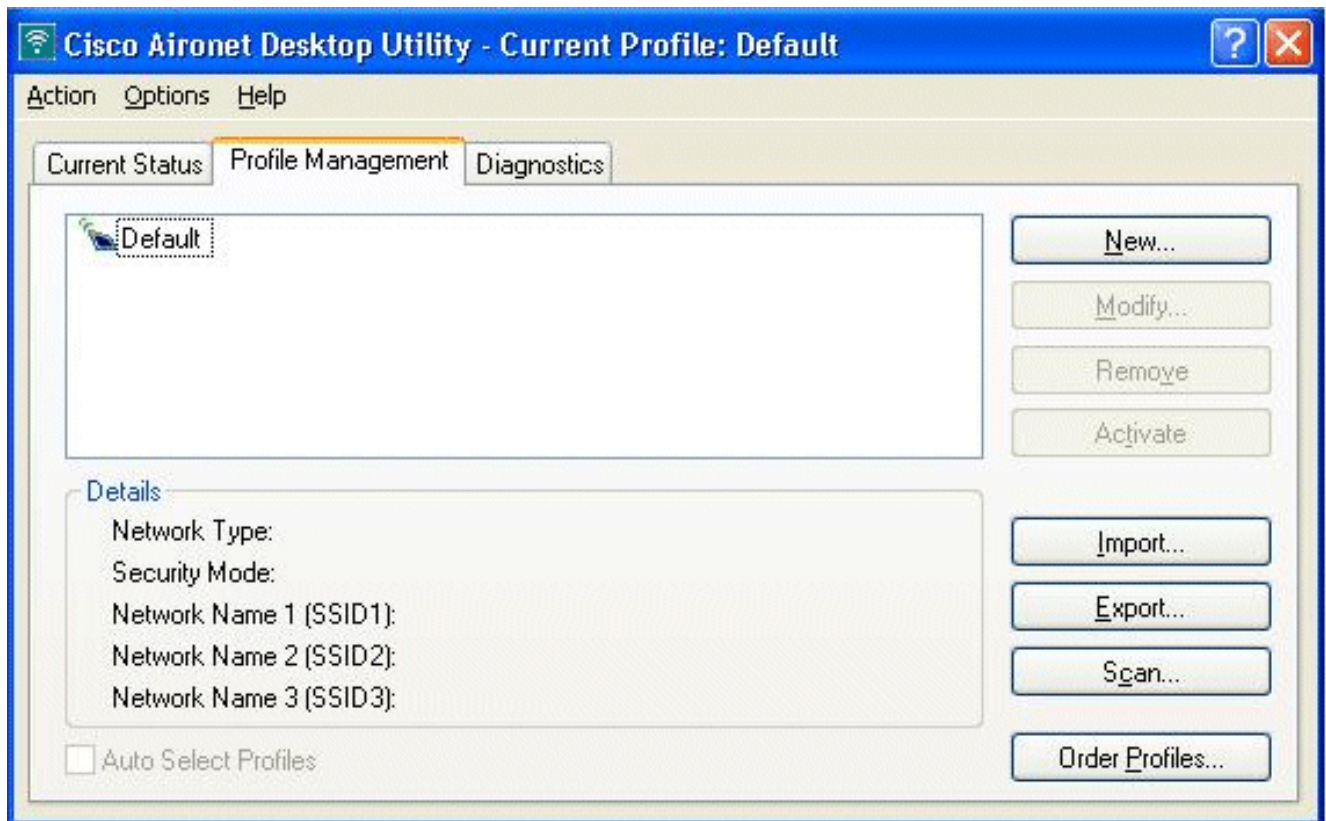
## [客户端身份验证过程](#)

### [客户端配置](#)

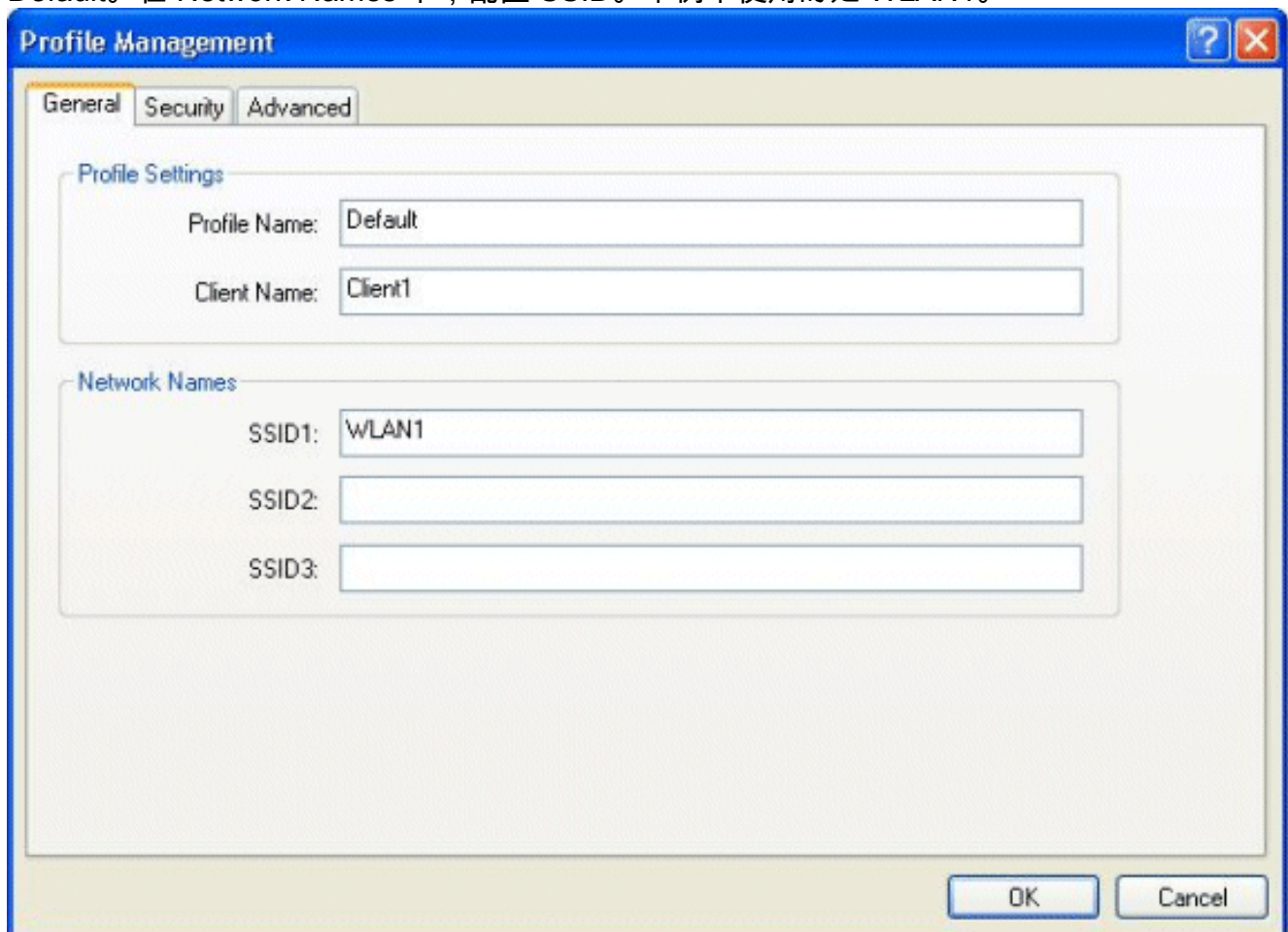
在本例中，我们使用 Cisco Aironet Desktop Utility 执行 Web 身份验证。执行这些步骤以便配置 Aironet Desktop Utility。

1. 从“开始”> Cisco Aironet > Aironet Desktop Utility 中打开 Aironet Desktop Utility。
2. 单击 Profile Management 选项卡。

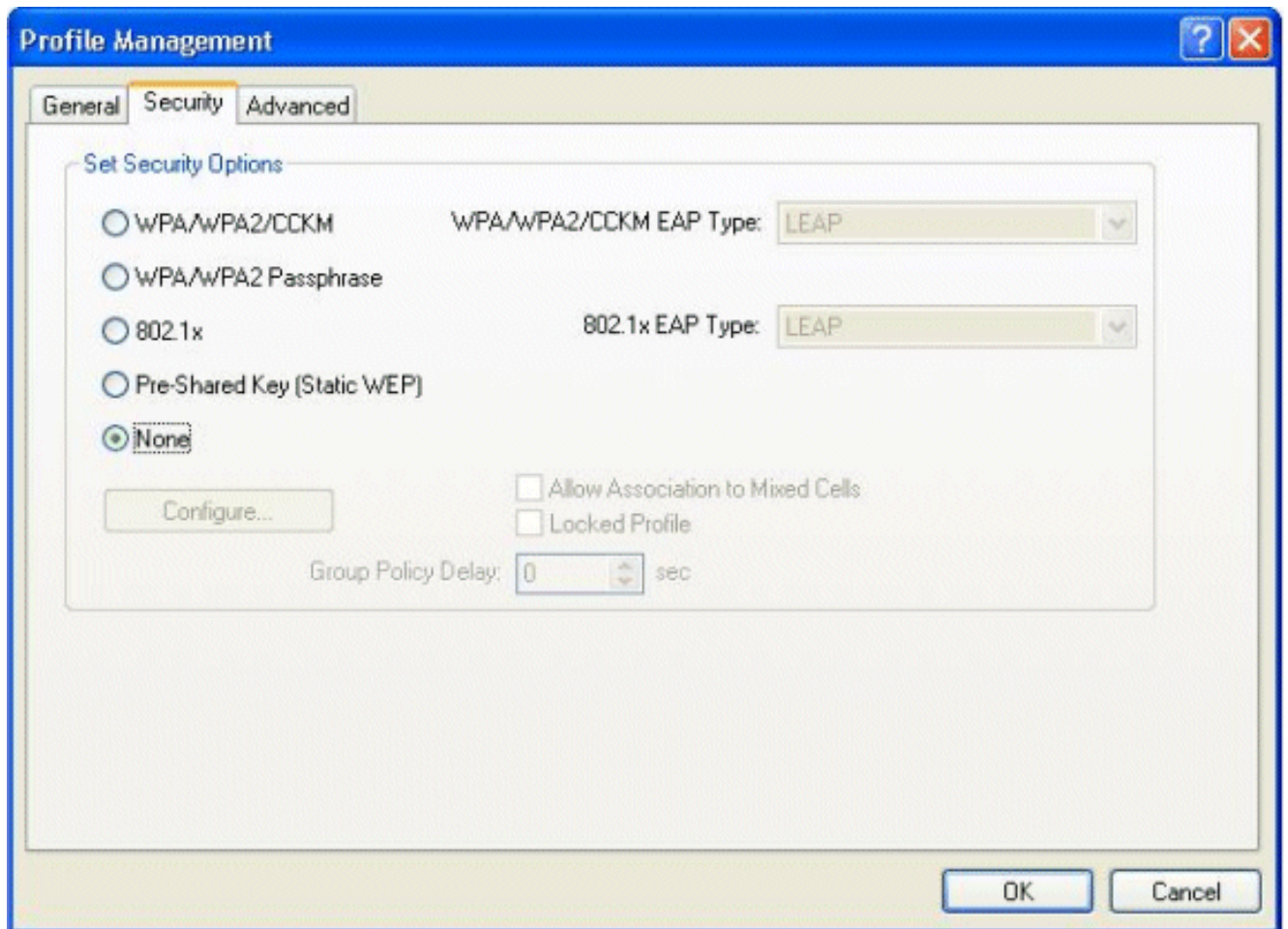




3. 选择 **Default profile**，并单击 **Modify**。点击**一般**选项。配置配置文件名称。本例中使用的是 *Default*。在 **Network Names** 下，配置 SSID。本例中使用的是 *WLAN1*。

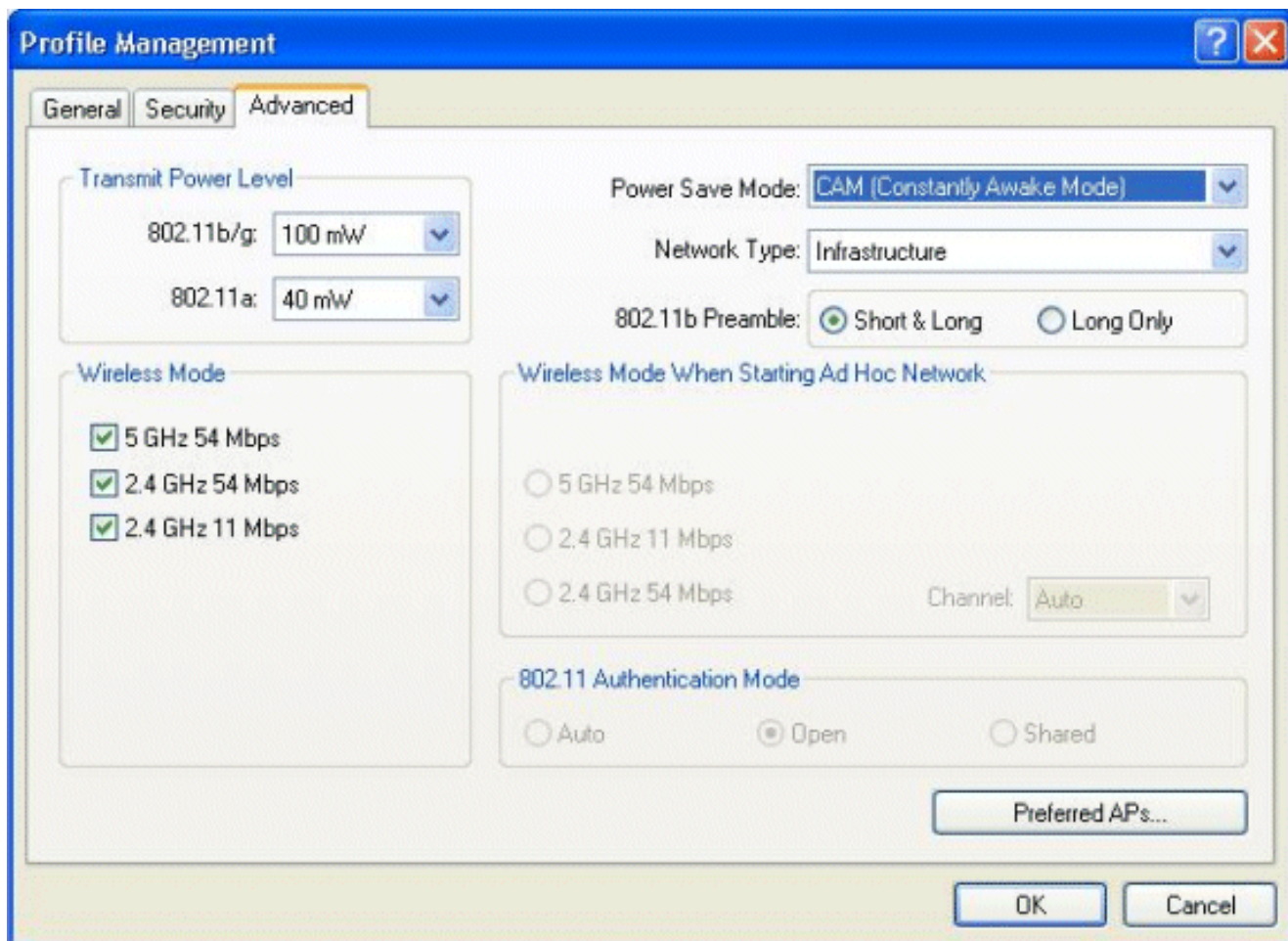


**注意：** SSID 区分大小写，并且应该与 WLC 上配置的 WLAN 相匹配。点击**安全**选项。请选择 **None** 作为 Web 身份验证的安全性。



点击高级选项卡。在 **Wireless Mode** 菜单下，选择无线客户端与 LAP 通信的频率。在 **Transmit Power Level** 下，选择 WLC 上配置的电源。保留节电模式的默认值。选择 **Infrastructure** 作为网络类型。将 802.11b 前导码设置为 **Short & Long** 以获得更好的兼容性。单击 **Ok**。



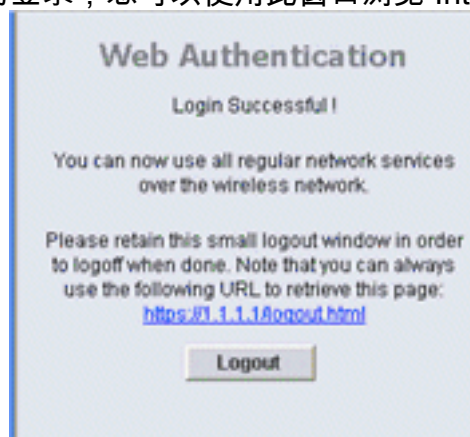


4. 一旦在客户端软件上配置了配置文件，客户端将顺利地关联并将收到为管理接口配置的 VLAN 池中的一个 IP 地址。

## 客户端登录过程

此部分说明客户端登录如何发生。

1. 打开浏览器窗口并输入所有 URL 或 IP 地址。这将从 Web 身份验证页转到客户端。如果控制器运行任何早于 3.0 的版本，则用户必须输入 `https://1.1.1.1/login.html` 才能显示 Web 身份验证页。此时将显示安全警报窗口。
2. 单击 **Yes** 以继续操作。
3. 当登录窗口出现时，请输入在 RADIUS 服务器上配置的用户名和密码。如果登录成功，您将看到两个浏览器窗口。较大的窗口表示您已成功登录，您可以使用此窗口浏览 Internet。完成



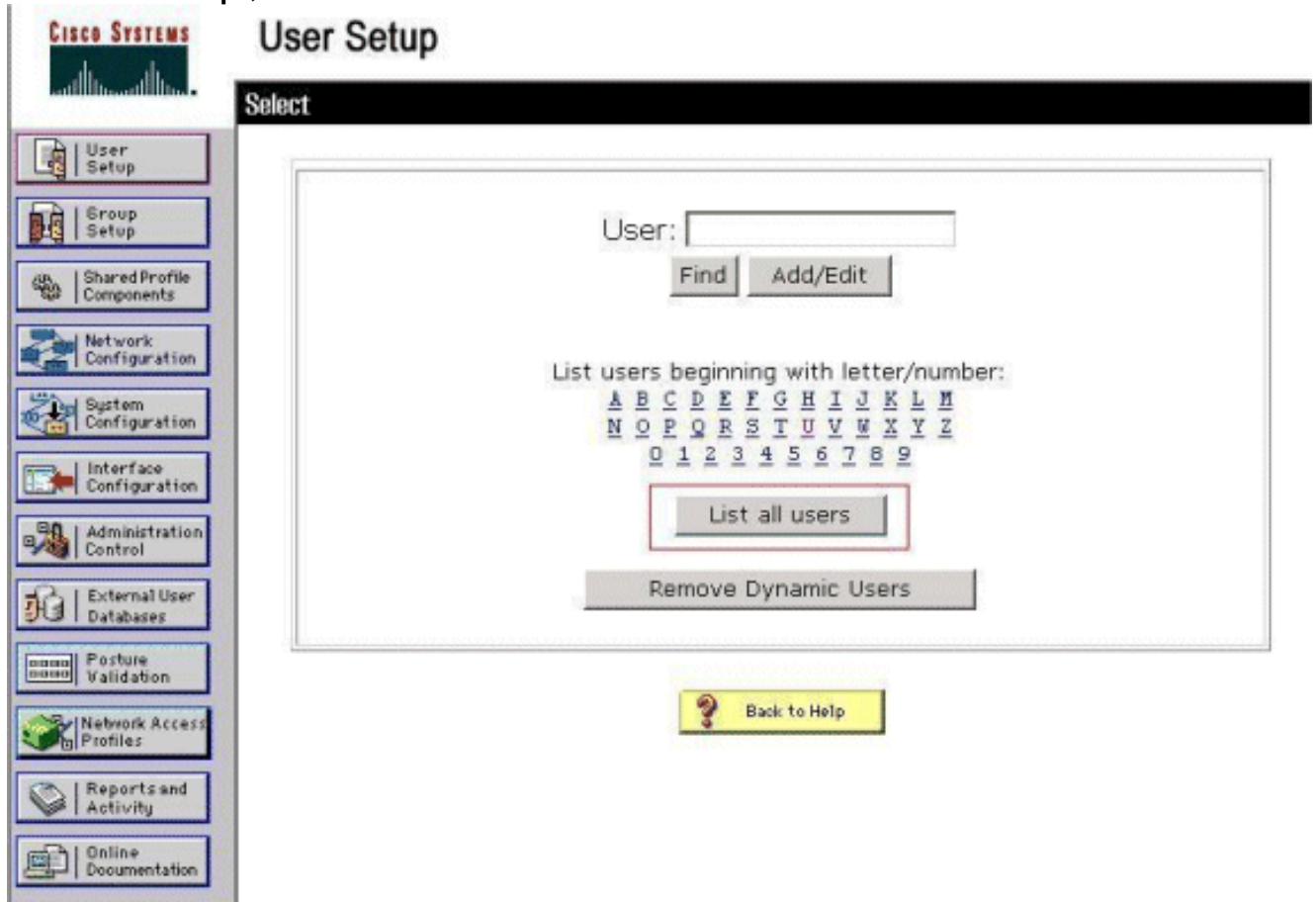
对访客网络的使用时，可使用较小的窗口注销。

## 验证

为使 Web 验证成功，您需要检查设备是否以适当的方式进行了配置。此部分说明如何验证过程中使用的设备。

### 验证 ACS

1. 单击 **User Setup**，然后在 ACS GUI 上单击 **List All Users**。



确保用户的状态为 *Enabled*，并且默认组已映射到用户。

User List			
User	Status	Group	Network Access Profile
<a href="#">user1</a>	Enabled	Default Group (2 users)	(Default)

2. 单击 **Network Configuration** 选项卡，并在 **AAA Clients** 表中进行查找，以便验证 WLC 是否配置为 AAA 客户端。



**CISCO SYSTEMS** Network Configuration

Select

**AAA Clients**

AAA Client Hostname	AAA Client IP Address	Authenticate Using
wlc1	10.77.244.206	RADIUS (Cisco Airespace)

Add Entry Search

**AAA Servers**

AAA Server Name	AAA Server IP Address	AAA Server Type
TS-Web	10.77.244.196	CiscoSecure ACS

Add Entry Search

**Proxy Distribution Table**

Character String	AAA Servers	Strip	Account
(Default)	TS-Web	No	Local

Add Entry Sort Entries

Back to Help

## 验证 WLC

1. 单击 WLC GUI 中的 **WLAN** 菜单。确保用于 Web 身份验证的 WLAN 在页面上列出。确保 WLAN 的 Admin Status 为 *Enabled*。确保 WLAN 的安全策略显示 *Web-Auth*。

**CISCO** MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

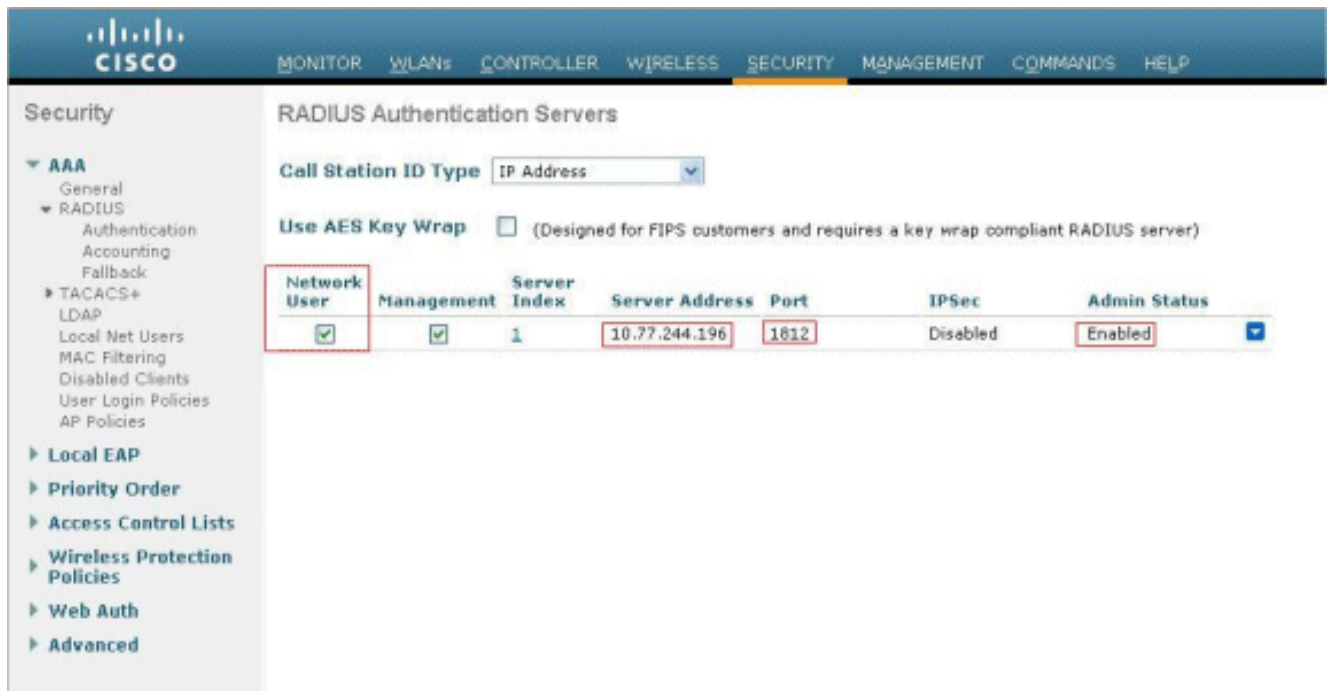
WLANs

WLANs

Advanced

Profile Name	Type	WLAN SSID	Admin Status	Security Policies
WLAN1	WLAN	WLAN1	Enabled	Web-Auth

2. 单击 WLC GUI 中的 **Security** 菜单。确保 Cisco Secure ACS (10.77.244.196) 在页面上列出。确保已选中 Network User 框。确保端口是 1812，并且 Admin Status 为 *Enabled*。



## 故障排除

Web 身份验证不成功有许多原因。文档[对无线 LAN 控制器 \(WLC\) 上的 Web 身份验证进行故障排除](#)将清楚地说明详细原因。

## 故障排除命令

**注意：** 使用这些 debug 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

通过 Telnet 连接到 WLC 并发出这些命令以对身份验证进行故障排除：

- **debug aaa all enable**

```

Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Successful transmission of Authentic
ation Packet (id 1) to 10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:01
Fri Sep 24 13:59:52 2010: 00000000: 01 01 00 73 00 00 00 00 00 00 00 00 00 00 0
0 00 ...s.....
Fri Sep 24 13:59:52 2010: 00000010: 00 00 00 00 01 07 75 73 65 72 31 02 12 93 c
3 66 .....user1....f
Fri Sep 24 13:59:52 2010: 00000030: 75 73 65 72 31
user1
Fri Sep 24 13:59:52 2010: ****Enter processIncomingMessages: response code=2
Fri Sep 24 13:59:52 2010: ****Enter processRadiusResponse: response code=2
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Access-Accept received from RADIUS s
erver 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 0
Fri Sep 24 13:59:52 2010: AuthorizationResponse: 0x12238db0
Fri Sep 24 13:59:52 2010:      structureSize.....89
Fri Sep 24 13:59:52 2010:      resultCode.....0
Fri Sep 24 13:59:52 2010:      protocolUsed.....0x0
0000001
Fri Sep 24 13:59:52 2010:      proxyState.....00:
40:96:AC:DD:05-00:00
Fri Sep 24 13:59:52 2010:      Packet contains 2 AVPs:
Fri Sep 24 13:59:52 2010:      AVP[01] Framed-IP-Address.....
.....0xffffffff (-1) (4 bytes)
Fri Sep 24 13:59:52 2010:      AVP[02] Class.....
.....CACS:0/5183/a4df4ce/user1 (25 bytes)
Fri Sep 24 13:59:52 2010: Authentication failed for user1, Service Type: 0

```

```

Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Applying new AAA override for station
00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Override values for station 00:40:96
:ac:dd:05
        source: 48, valid bits: 0x1
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

dataAvgC: -1, rTavgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                vlanIfName: '',
aclName:
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Unable to apply override policy for
station 00:40:96:ac:dd:05 - VapAllowRadiusOverride is FALSE
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Sending Accounting request (0) for s
tation 00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: AccountingMessage Accounting Start: 0x1500501c
Fri Sep 24 13:59:52 2010:         Packet contains 12 AVPs:
Fri Sep 24 13:59:52 2010:         AVP[01] User-Name.....
.....user1 (5 bytes)
Fri Sep 24 13:59:52 2010:         AVP[02] Nas-Port.....
.....0x00000002 (2) (4 bytes)
Fri Sep 24 13:59:52 2010:         AVP[03] Nas-Ip-Address.....
.....0x0a4df4ce (172881102) (4 bytes)
Fri Sep 24 13:59:52 2010:         AVP[04] Framed-IP-Address.....
.....0x0a4df4c7 (172881095) (4 bytes)

```

- **debug aaa detail enable**

失败的身份验证尝试在位于 **Reports and Activity > Failed Attempts** 处的菜单中列出。

## [相关信息](#)

- [无线局域网控制器Web身份验证配置示例](#)
- [对无线 LAN 控制器 \(WLC\) 上的 Web 身份验证进行故障排除](#)
- [与无线局域网控制器配置示例的外部Web认证](#)
- [在无线局域网控制器\(WLCs\)上使用LDAP的Web认证配置示例](#)
- [技术支持和文档 - Cisco Systems](#)