

无线局域网控制器 Web认证配置举例

文档编号: 69340

介绍

前提

要求

使用的设备

惯例

Web 方式认证

在控制器上配置 Web 方式认证

创建一个 VLAN 接口

添加 WLAN 实例

在 WLC 上配置 DHCP 及 DNS

重启 WLC

Web 认证下两种认证用户的方式

在你的 Windows 计算机上配置使用 Web 认证

客户端配置

客户端登录

内部 Web 认证配置的核对及排障

核对 ACS 配置

核对内部 Web 认证配置

ACS 排障

内部 Web 认证排障

在 WLAN 上没有配置认证服务器时 Web 认证依然向外部认证服务器发送认证请求

微软 IE 因为缓存重定向到 Web 认证登录页面

定制 Web 认证页面原则

定制 Web 认证成功或者 Web 认证登录页面

在 WLC 上定制 Web 认证成功或者 Web 认证登录页面

在 WCS 上定制 Web 认证成功或者 Web 认证登录页面

在 WLAN 上分配登录，登录失败，登出页面

基于 802.1x 认证的有条件的 Web 重定向

相关信息

介绍

本文介绍了如何配置思科4400系列无线局域网控制器（WLC）支持web方式的客户端认证。

前提

要求

本文需要你已经掌握 4400WLC 的初始化配置。

使用的设备

本文的内容是基于以下的硬件平台与软件版本的：

- 4400系列无线局域网控制器，软件版本为5.0.148.0
- 思科4.2版本的ACS软件，安装在微软Windows2003服务器上
- 思科Aironet 1230系列轻型无线接入点
- 思科Aironet 802.11 a/b/g CardBus无线网卡，软件版本为3.6

本文的内容是基于特殊的实验室环境而产生的。所有设备都是从默认配置开始配置的。如果你的网络正在运行中，请确保理解这些配置可能对你的网络造成的潜在影响。

惯例

对更多文档惯例的信息，请参见思科技术提示惯例。

Web 方式认证

Web方式认证是一个三层的安全特性，在无线客户端输入正确的用户名口令之前，控制器不接受该用户的IP数据（除了DHCP相关的数据包）。Web认证可以通过WLC本地认证，也可以通过RADIUS服务器。通常在部署访客网络时，使用Web方式认证。典型的部署模式包括“热点”区域，例如T-Mobile或者星巴克。

Web方式认证提供了不需要802.1x认证请求方或者客户端工具的简单的认证方式。记住Web方式认证不提供数据加密。Web认证通常被用在“热点”或者仅考虑连接性的园区环境。

本文中创建了一个新的VLAN接口和一个新的用作Web认证的WLAN。这个VLAN接口被分配到这个WLAN上，因此接入这个WLAN的用户是在一个独立的子网。在那些你不希望用独立子网的场合，你可以把WLAN关联到Management 接口。本文中控制器的Web认证配置包含了新建一个VLAN接口的过程。

在控制器上配置 Web 方式认证

下文介绍了如何在控制器上配置Web方式的认证。

本文使用以下IP地址：

- 无线局域网控制器的IP地址是10.77.244.204。

- ACS服务器的地址是10.77.244.196。

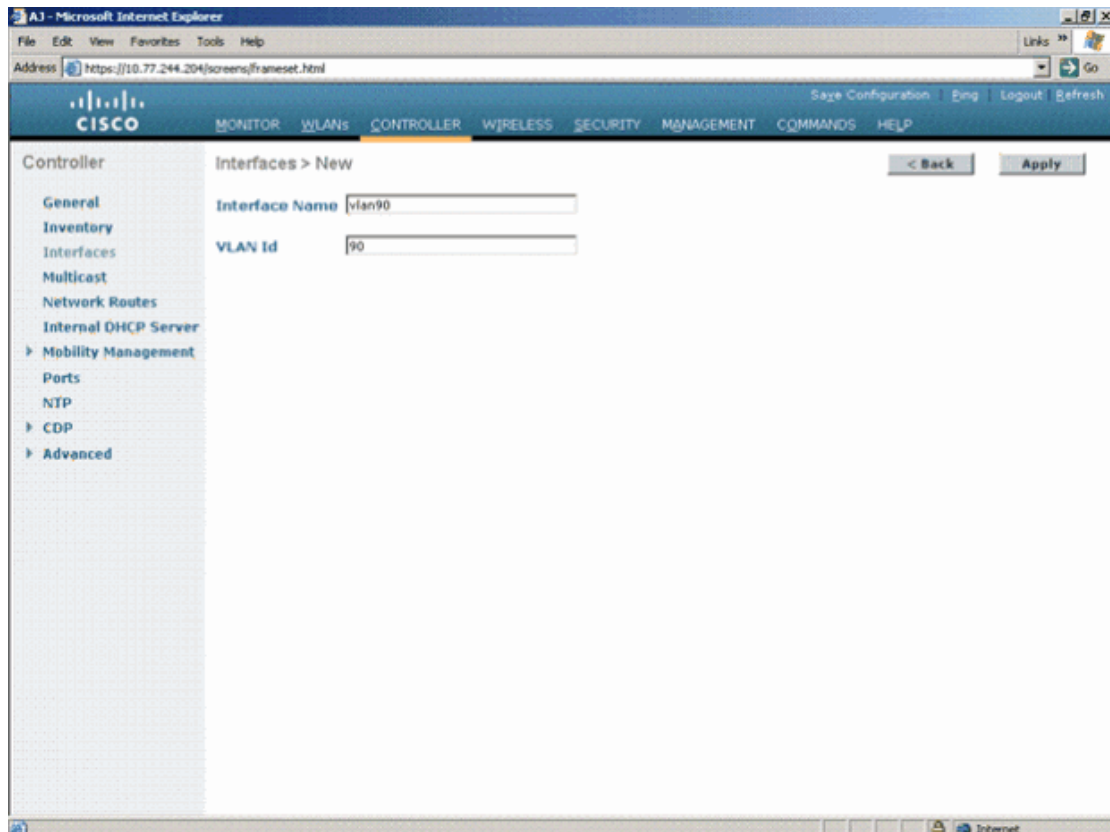
创建一个 VLAN 接口

完成以下步骤：

1. 在控制器的主页上，选择最上方的**Controller**菜单，选择左边的**Interfaces** 栏，点击窗口右上方的**New**。

图1的窗口出现了。本例中接口名字是vlan90，VLAN号是90：

图 1



2. 点击**Apply**，创建该VLAN接口。
一个新的窗口出现，需要你填入相关信息。

3. 本文采用以下参数：

- IP Address: 10.10.10.2
- Netmask: 255.255.255.0 (24 bits)
- Gateway: 10.10.10.1
- Port Number: 2
- Primary DHCP Server: 10.77.244.204

注意：这个参数应该填写DHCP服务器地址。在本例中WLC的管理地址被用来当作DHCP服务器的地址，因为在WLC启用的DHCP功能。

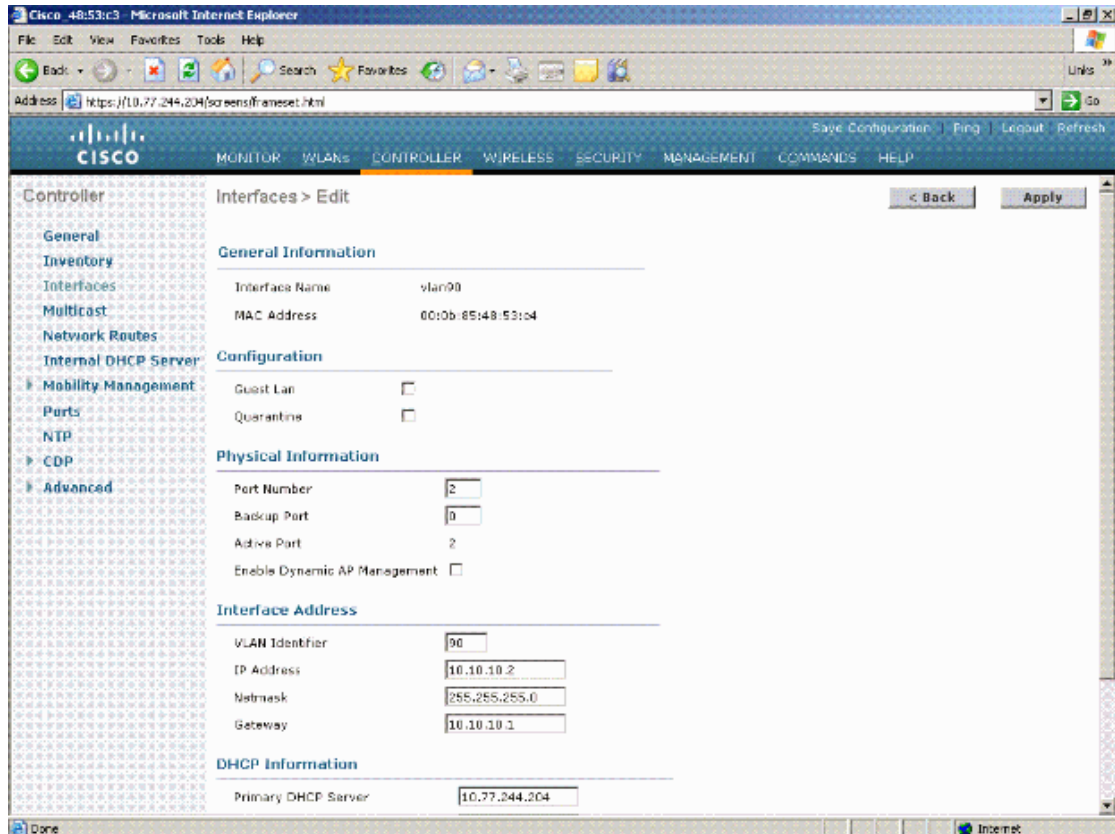
- Secondary DHCP Server: 0.0.0.0

注意：本文不使用dier1DHCP服务器，所以使用0.0.0.0。如果你有第二台DHCP服务器，需要在这里填写地址。

- ACL Name: None

图 2 显示了这些配置：

图 2



4. 点击 **Apply** ，保存配置。

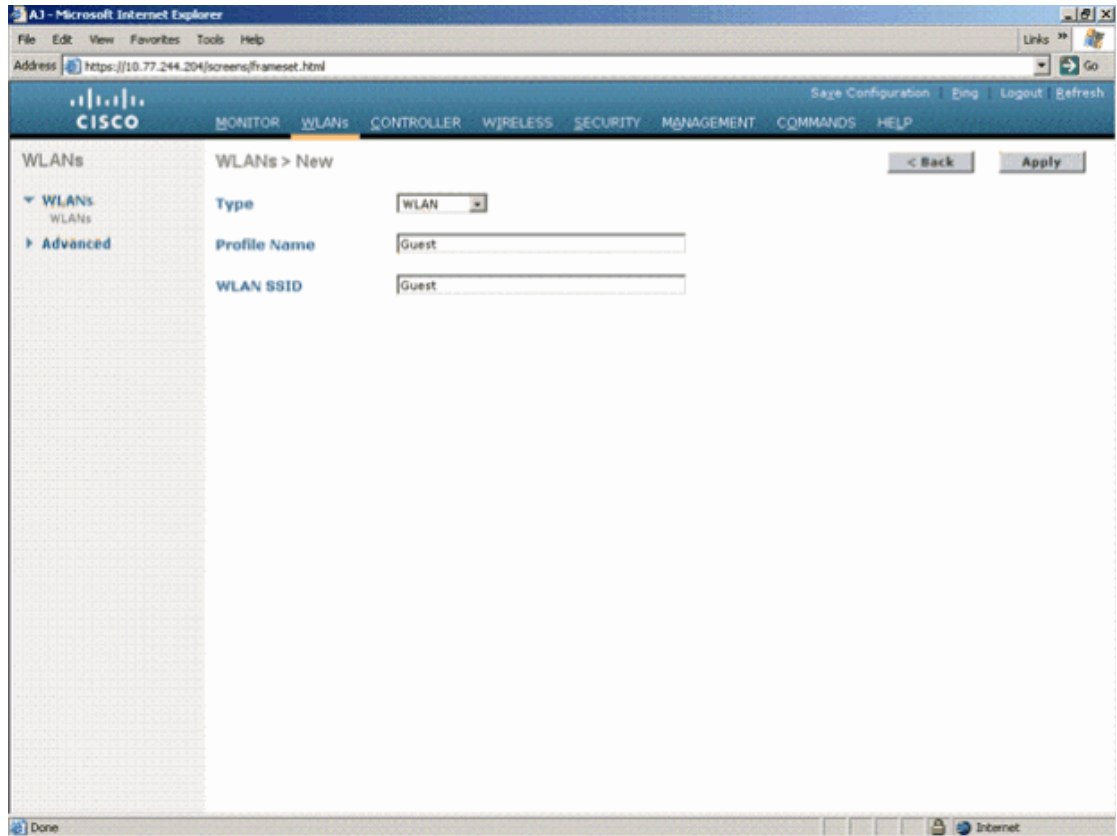
添加 WLAN 实例

现在一个VLAN接口已经配置好，你需要提供一个WLAN/SSID来支持Web认证的用户。通过以下方式，创建一个新的 WLAN/SSID：

1. 打开WLC页面，点击最上方**WLAN**菜单，点击右上方的**New**。会弹出类似图3的画面。

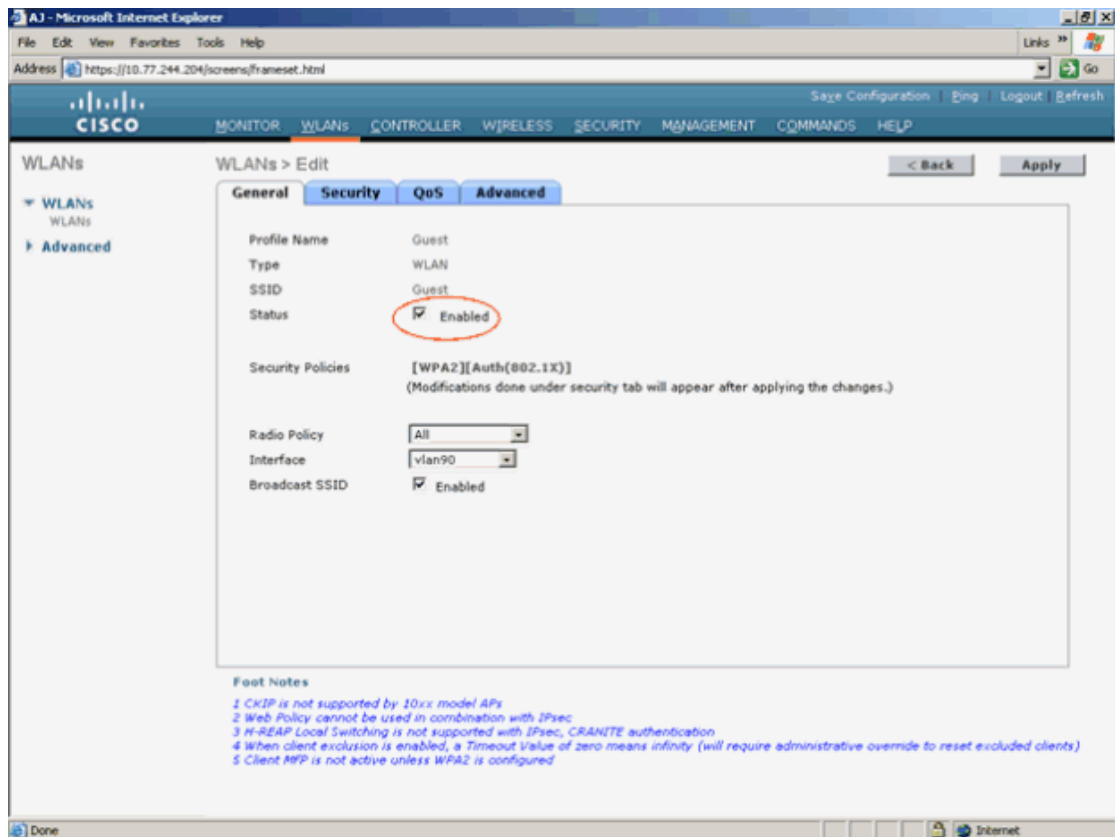
将类型选为**WLAN**。为这个WLAN SSID选择一个名字。本例中Profile 和WLAN都是**Guest**。

图 3



2. 点击**Apply**。
出现一个新的WLAN > Edit窗口，如图4所示。

图 4

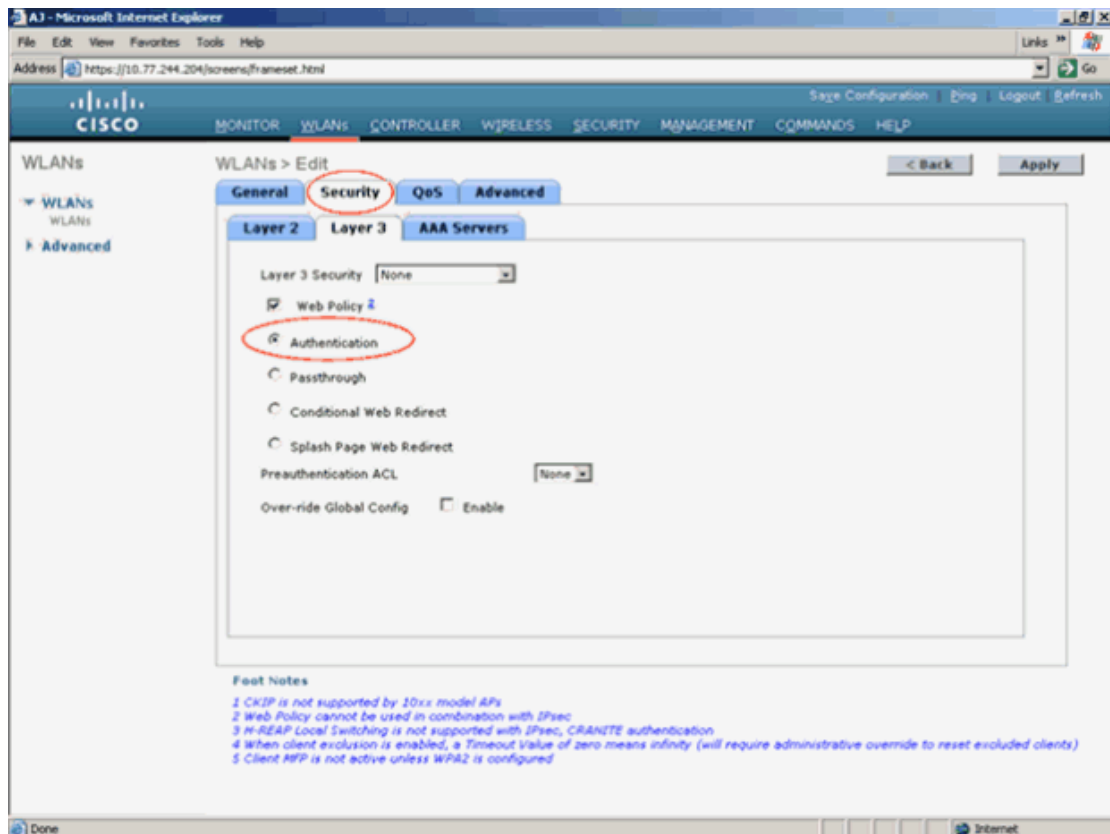


3. 勾选WLAN的状态栏，激活该WLAN。在接口栏，选择先前创建的VLAN接口。在本例中，接口的名字是vlan90。

注意：其他参数不做修改，都是初始设置。

4. 点击Security栏。出现图5。

图 5



通过以下步骤，完成Web认证配置：

a) 点击Layer 2栏，选择**None**。

注意：当某个WLAN的二层安全策略使用802.1x or WPA/WPA2时，你的三层安全策略不可以配置成web passthrough。关于控制器上二层和三层安全策略的兼容问题，参见Wireless LAN Controller Layer 2 Layer 3 Security Compatibility Matrix一文。

b) 点击Layer 3 栏。如图5所示，勾选Web Policy框，选择**Authentication** 选项

c) 点击Apply，保存配置。

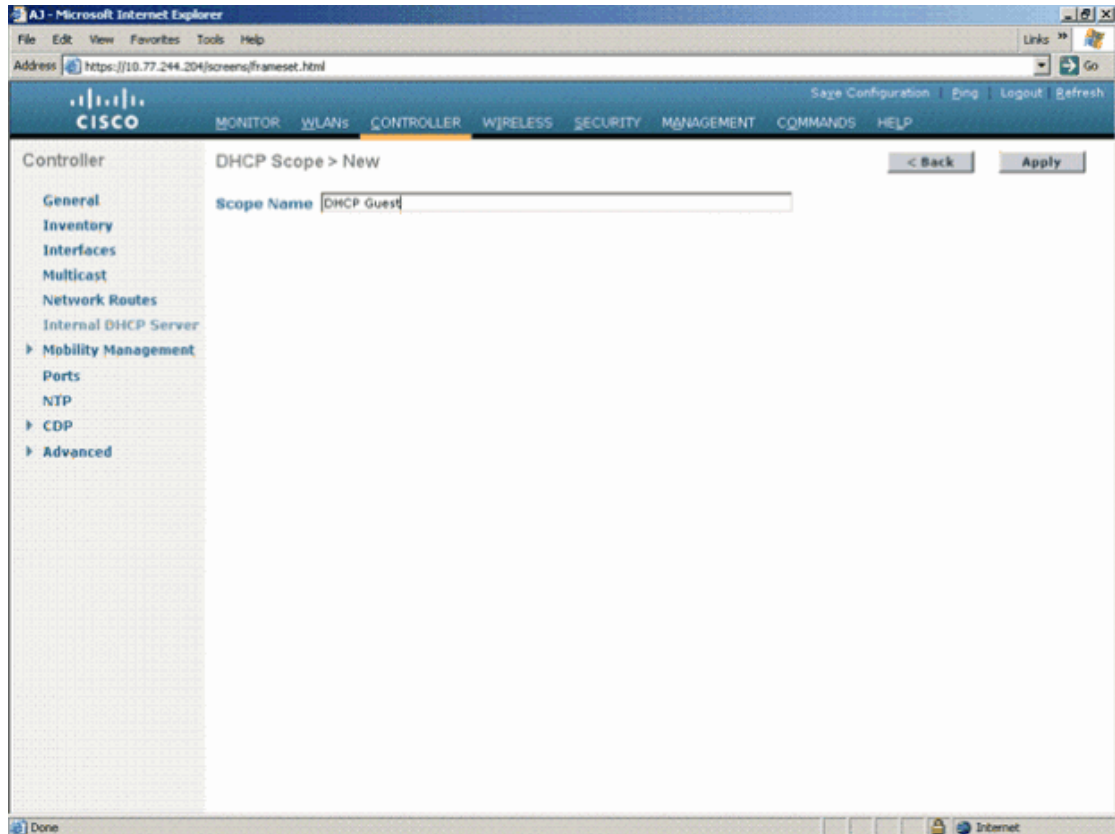
d) 这个时候你回到了WLAN概要页面。确认你的Web认证选项在SSID Guest下已经配置。

在 WLC 上配置 DHCP 及 DNS

完成以下步骤：

1. 点击菜单页面上方的**Controller** 。
2. 点击菜单左面的Internal DHCP Server。
3. 点击**New**，创建一个DHCP池。
4. 键入你需要分配给客户端的DHCP地址池。如图6所示。

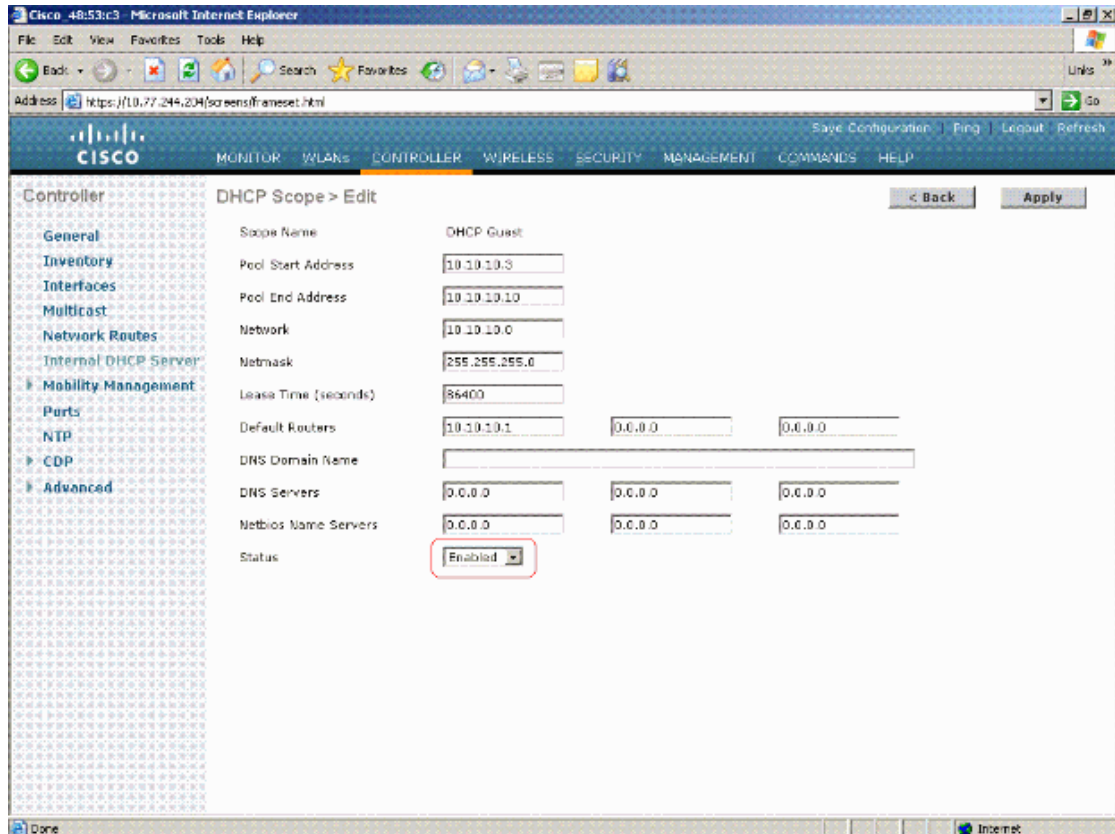
图 6



5. 点击Apply.
6. 出现DHCP Scope > Edit窗口.
7. 键入地址池的起始及终止地址。。在本例中，DHCP地址池是从10.10.10.3到10.10.10.10。
8. 键入默认网关的地址，是10.10.10.1。
9. 键入DNS域名和DNS服务器的地址。确认**Status**是激活的。

图 7 给了一个例子：

图 7



10. 点击 Apply。

重启 WLC

由于不能在系统工作的时候完成一个或者更多的WLAN上的改变，你需要重启WLC。修改需要在启动前或者启动中完成。完成以下步骤来重启WLC：

1. 在控制器的主界面上，选择菜单最上方的**Commands**。
2. 在新的窗口下，选择左边菜单上的**Reboot**。
如果在你的配置中有未保存的部分，你需要保存配置然后重启。
3. 点击**Save and Reboot**，保存配置然后重启设备。
4. 通过console连接监控设备的重启过程。
当WLC启动完毕，你可以创建你的Web认证用户了。

Web 认证下两种认证用户的方式

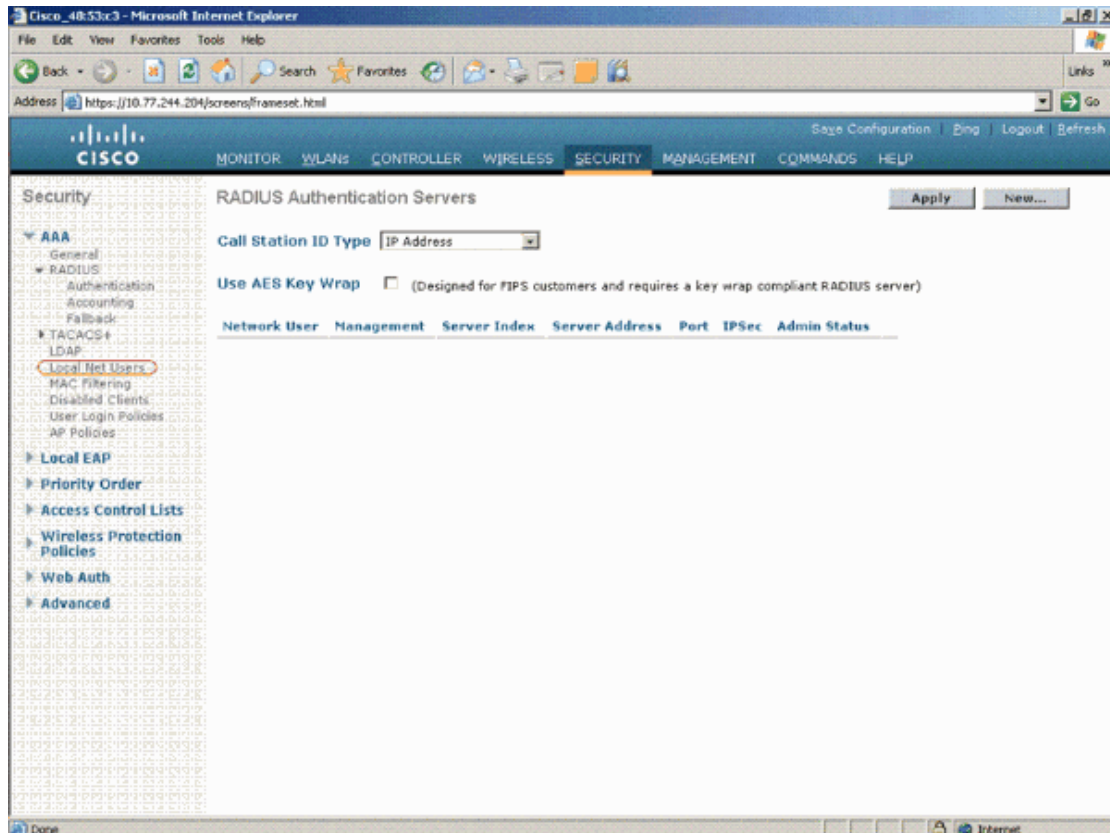
当你使用Web认证的时候，有两种认证用户的方式。本地认证允许你使用WLC的用户去认证。你也可以使用RADIUS服务器认证用户。配置WLC的本地认证，完成以下步骤：

本地认证

用户名和密码存放在控制器的本地数据库。用户通过WLC的这个数据库来认证。以下步骤描述了如何在WLC上创建用户名和密码：

1. 在菜单上方点击**Security**，进入WLC的安全配置窗口。
 2. 在左边AAA菜单里，选择**Local Net Users**
- 图 8给出了例子。

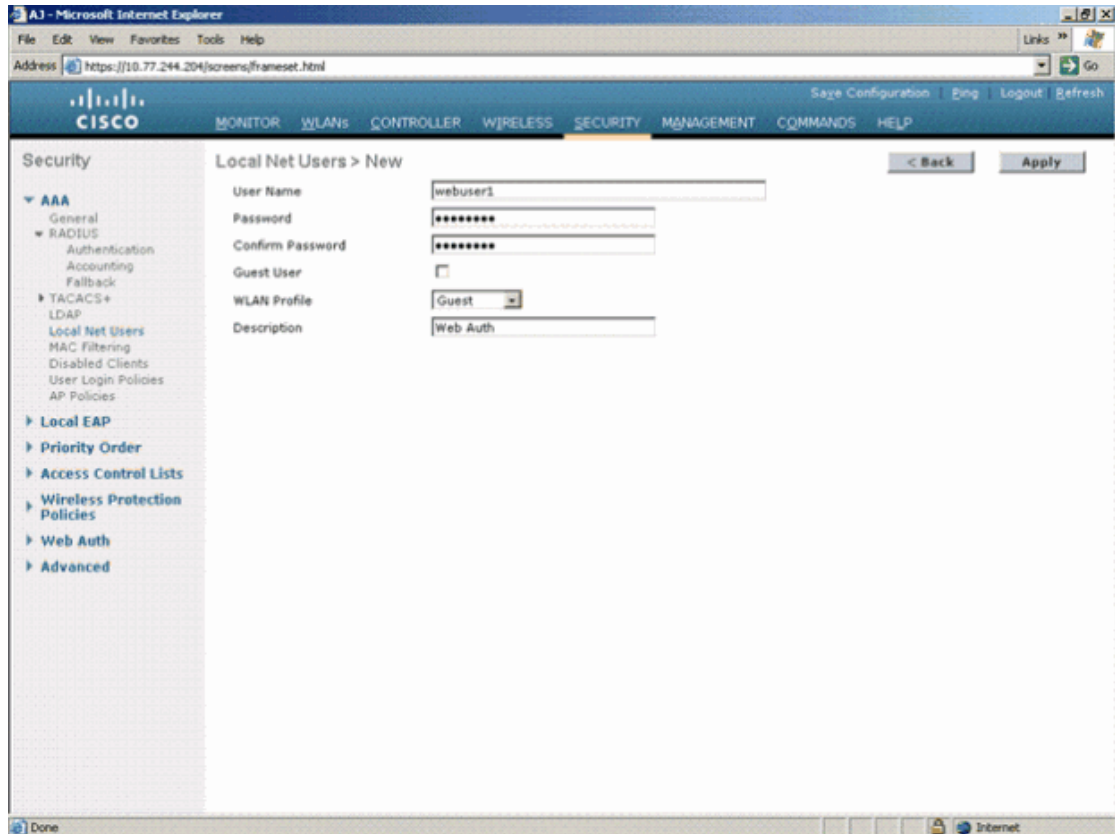
图 8



3. 点击右上方的**New**，创建一个新的用户。
会出现一个新的窗口，需要你填写用户名和密码。
4. 填入用户名和密码，确认密码。
本例中创建的用户是 *webuser1*。
5. 核对你的用户是否分配到正确的WLAN上。该动作确保这个用户只能在特定的WLAN认证使用。
本例中，WLAN Profile是， *Guest*，该WLAN用作Web方式的认证。
6. 如果你需要，添加一个描述。
本例中使用 *Web Auth*。
7. 点击**Apply**，保存用户配置。

图 9 给出了例子：

图 9



RADIUS 服务器的 Web 认证

本文使用安装在Windows2003服务器上的ACS作为RADIUS服务器。你可以使用你网络中部属的可用的RADIUS服务器。

注意: ACS可以在Windows NT或者Windows 2000服务器上安装。关于在思科网站下载ACS，通过Software Center (Downloads) – Cisco Secure Software (限注册用户使用)。你需要一个思科网站的帐号去下载软件。

当Web认证是通过RADIUS服务器的时候，第一个认证的询问是发给WLC本地的。如果WLC没有回答，第二个询问发到RADIUS服务器。ACS建立部分介绍了如何配置ACS。你需要有DNS和RADIUS服务器。

ACS 建立

下文将告诉你如何建立一个ACS作为RADIUS服务器。

在你的服务器上建立ACS，然后通过以下步骤来创建认证用户：

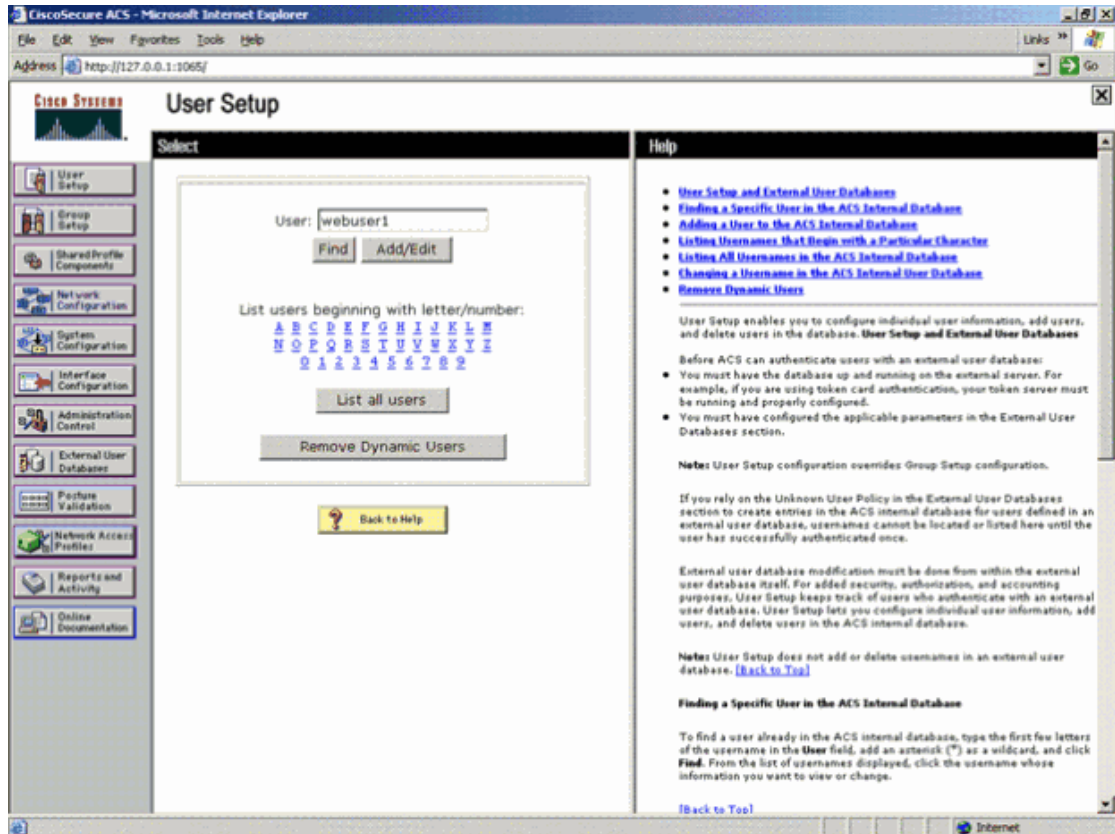
1. 当ACS问你是否需要打开ACS页面来配置的时候，点击**yes**。

注意: 在你安装完ACS后，在你的桌面会有一个快捷图标。

2. 在左边菜单里，点击**User Setup**。

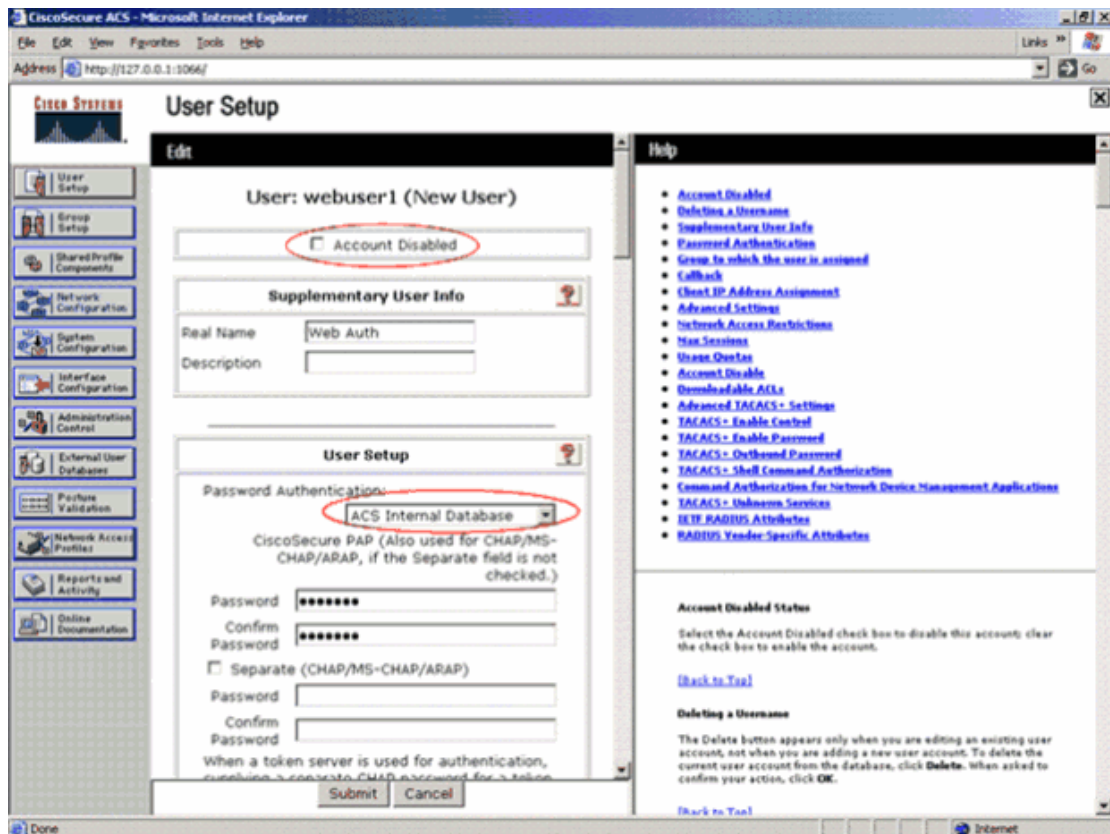
这个动作把你带到了用户建立的页面，如图10所示。

图 10



- 键入你想用来Web认证的用户，点击Add/Edit。
在用户建立之后，会出现另一个窗口，如图11所示。

图 11



4. 确认最上方的**Account Disabled**框没有勾选，如图11所示。
5. 在Password Authentication选项里，选择ACS Internal Database。
6. 输入2次密码。
7. 点击 Click Submit。

在思科 WLC 上输入 RADIUS 服务器信息 Enter

完成以下步骤：

1. 在上方的菜单中点击**Security**。
2. 在左边菜单里点击**Radius Authentication**。
3. 点击**New**，键入ACS/RADIUS服务器的地址。本例中，ACS的地址是**10.77.244.196**。
4. 键入Radius服务器的共享密钥。确保密钥和在Radius服务器上为WLC配置的密钥一致。
5. Port number保持默认，1812。
6. 确保**Server Status**选项是Enabled。
7. 勾选**Network User Enable** 框，这样Radius服务器就用来认证无线网络的用户了。
8. 点击**Apply**。

图 12 给了一个例子：

图 12

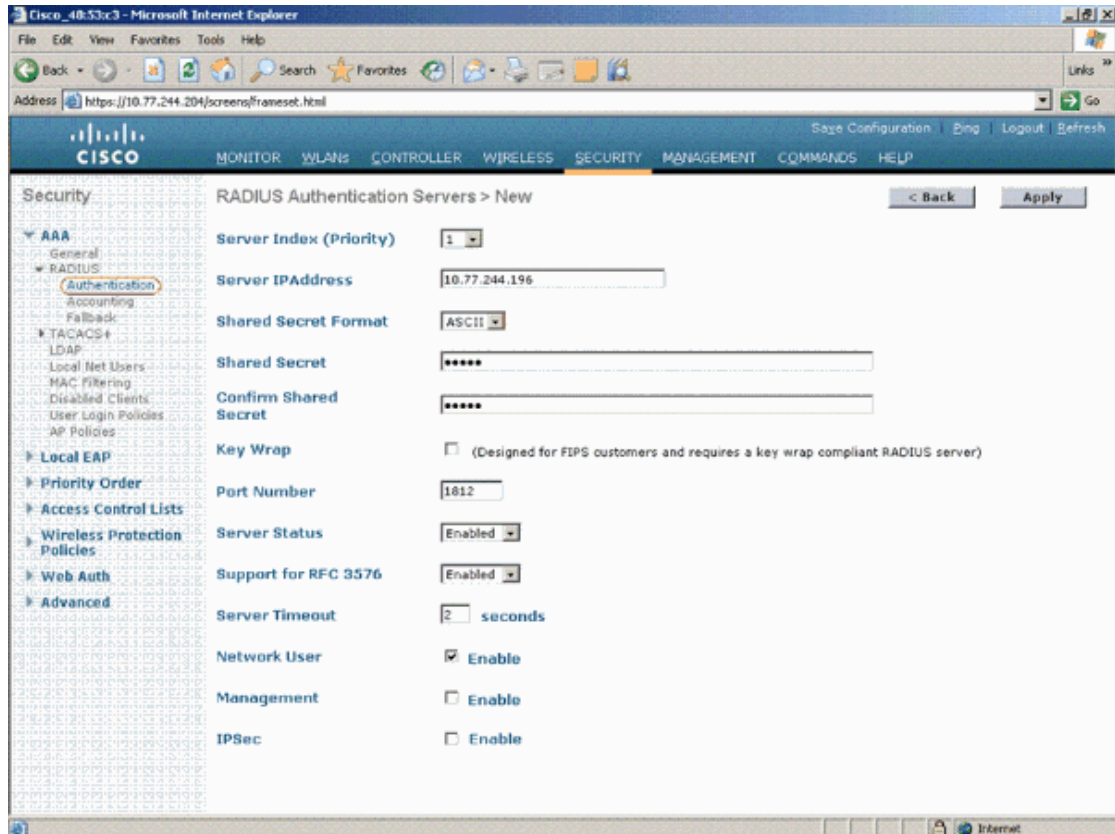
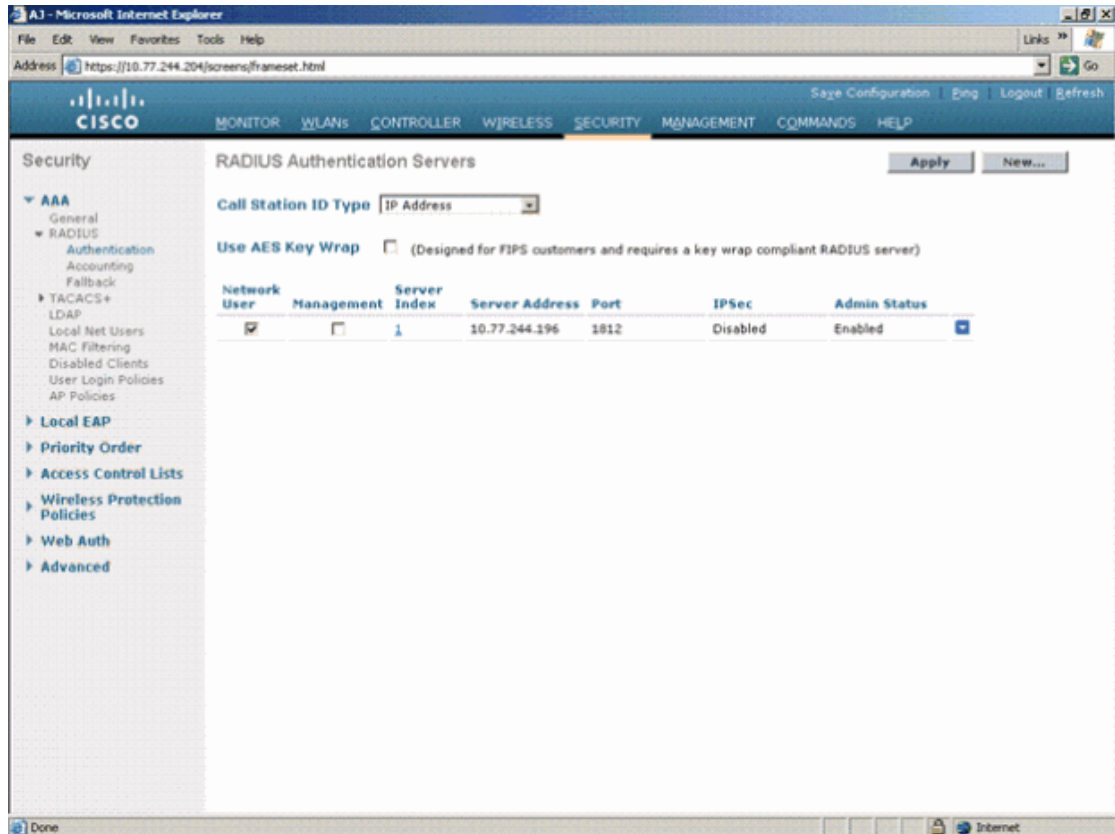


图 13 显示了一个配置好的RADIUS 服务器。确保Network User框是勾选的，Admin Status 是Enabled。

图 13

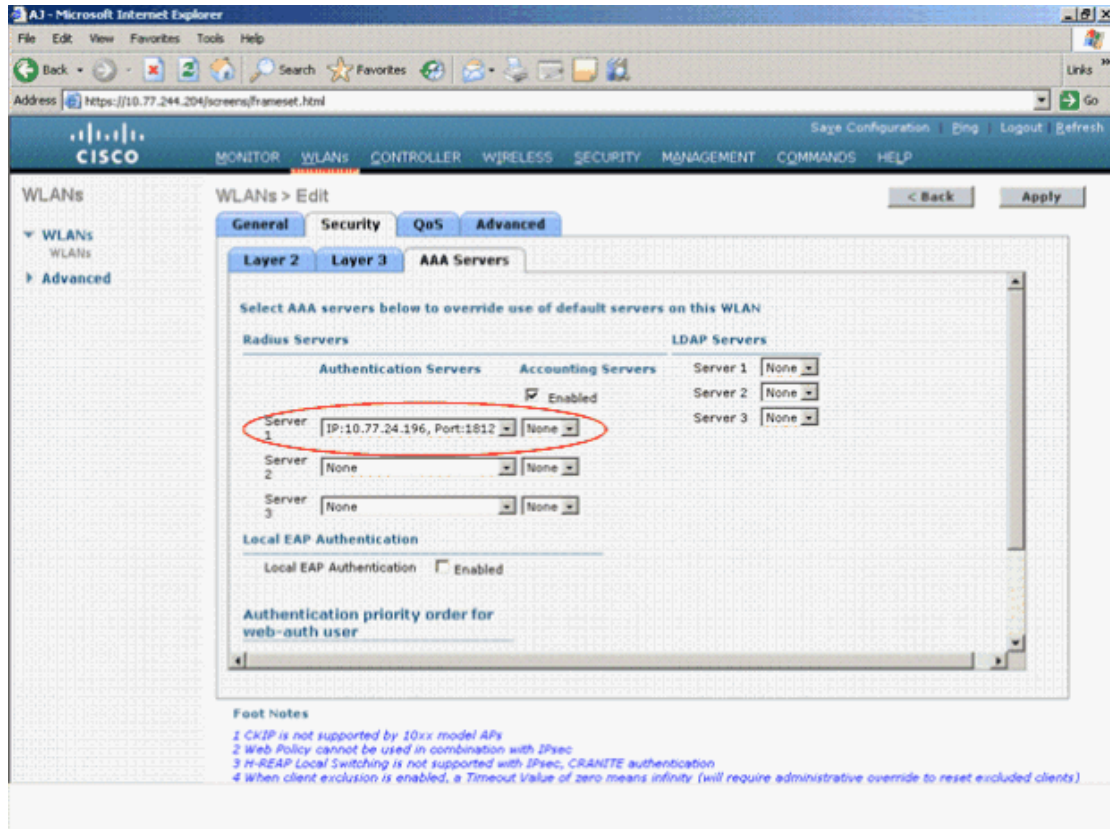


配置 WLAN 上的 RADIUS 服务器

到目前，RADIUS服务器已经在WLC配置好了，你需要在WLAN上使用这个RADIUS服务器作Web认证。通过以下步骤，完成WLAN上RADIUS服务器的配置。

1. 打开WLC页面，点击**WLANs**。该页面显示了WLC上已配置的WLAN的列表。点击**Guest**这个WLAN。
2. 在**WLANs>Edit**页面，点击**Security**菜单。点击安全菜单下的**AAA Servers** 一栏。如图14所示，选择Radius服务器，本例中为10.77.244.196。

图 14



3. 点击 Apply。

在你的 Windows 计算机上配置使用 Web 认证

一旦WLC完成了配置，客户端需要正确配置Web方式的认证。下文介绍了如何在Windows系统上配置Web认证。

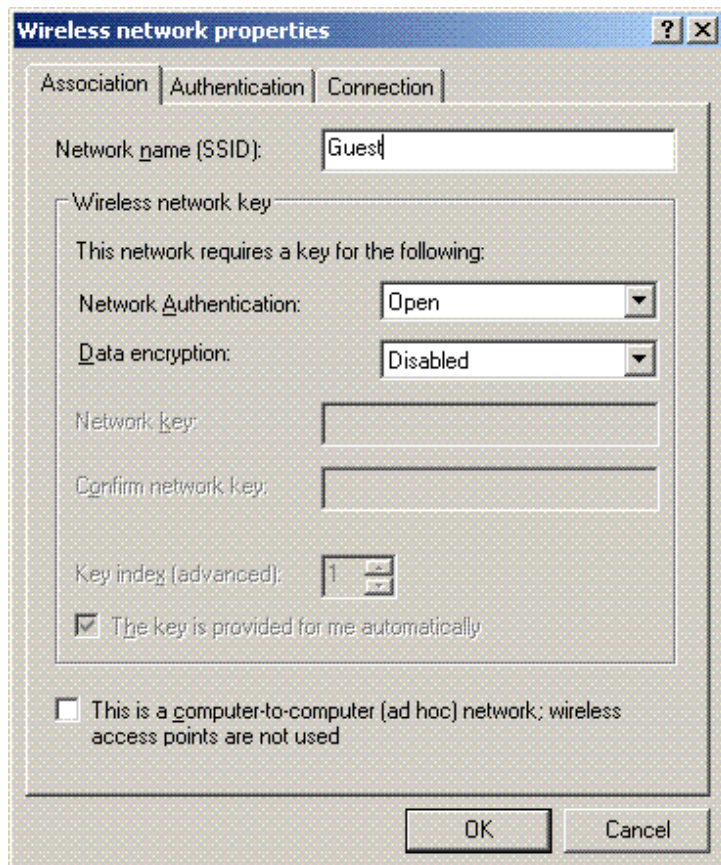
客户端配置

微软无线客户端配置基本保持不变。你只需要添加相应的WLAN/SSID配置。完成以下步骤：

1. 通过Windows的**Start**菜单，选择**Settings > Control Panel > Network and Internet Connections**。
2. 点击**Network Connection**图标。
3. 右键单击**LAN Connection**图标，选择**Disable**。
4. 右键单击**Wireless Connection**图标，选择**Enable**。
5. 再次右键单击**Wireless Connection**图标，选择**Properties**。
6. 从无线网络连接属性窗口，点击**Wireless Networks**栏。
7. 在优选网络中，点击**Add**，添加Web认证的SSID。
8. 在关联栏下，键入网络名称 (WLAN/SSID)。

图 15 给出了一个例子：

图 15



注意：数据加密选项默认为Wired Equivalent Privacy (WEP) 。为了支持Web认证，关闭数据加密。

9. 点击窗口底部的**OK**，保存配置。

当你连接这个WLAN的时候，你会在优选网络框中看见一个信标的图标。

图16 显示了一个成功的Web认证的连接。WLC分配给你的Windows客户端一个IP地址。

图 16



注意：如果你的无线客户端同时也是以VPN终端，同时你配置WLAN的Web认证的特性，除非通过了Web认证，不然VPN隧道不会建立。只有通过了Web认证，VPN隧道才会建立。只有那个时候，VPN隧道建立才会成功。

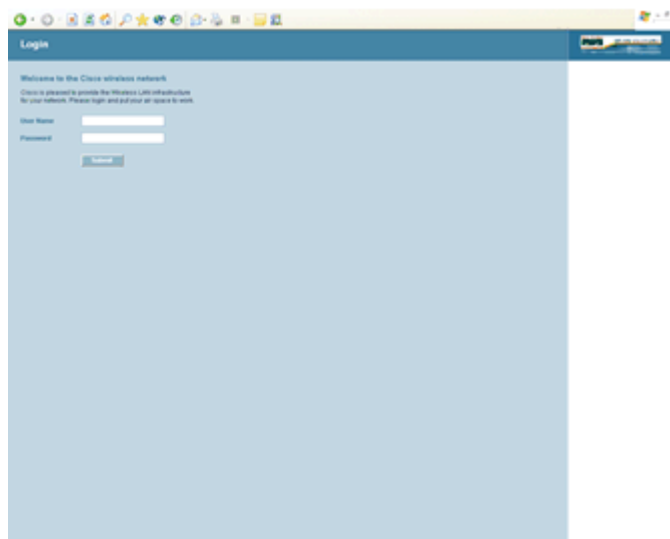
注意：在成功的登录之后，如果无线客户端并没有和其他设备通信，该客户端会在过了WLAN上配置的会话超时周期后断开关联。当这样的情况发生后，该客户端处在**Webauth_Reqd**的状态，除非你断开连接重新打开浏览器建立连接，不然无法恢复。当会话超时周期到达之后，这个是预计的行为。

客户端登录

完成以下步骤：

1. 打开浏览器，键入你所设置用来本地认证的virtual IP地址。
使用<https://1.1.1.1/login.html>。
这个步骤在3.0版本以前是非常重要的。在之后的版本，打开任何URL都会把你重定向到web认证的页面。同时，在所有最近的控制器软件版本中，支持通过http的web认证登录。这个和控制器管理登录联系在一起。为了支持这个功能，需要关闭https登录，只打开http管理。如果现在你打开web认证，将使用http方式的登录。
出现一个安全告警窗口。
2. 点击**Yes**。
3. 当登录窗口出现后，键入所创建的本地用户的用户名和密码。
如果登录成功，你会看见两个浏览器窗口。大的表示登录成功，你可以用这个窗口浏览internet。当你的访客接入完成后，使用小的窗口登出。
图 17 显示了一个成功的web认证的重定向。

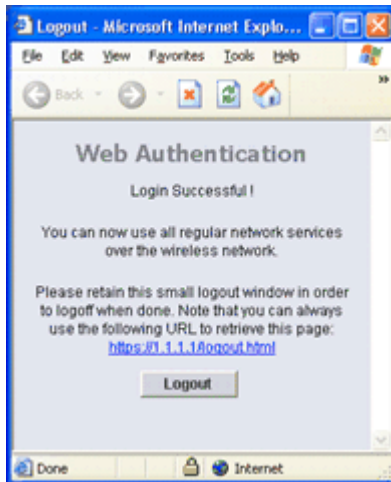
图 17



注意：这个默认的Web认证页面是由思科提供的。这个页面也可以定制。如何定制页面，参见本文订制Web认证通过或者Web 认证登录页面的部分。

图18 显示了当认证在ACS中发生时的一个登录成功的窗口

图 18

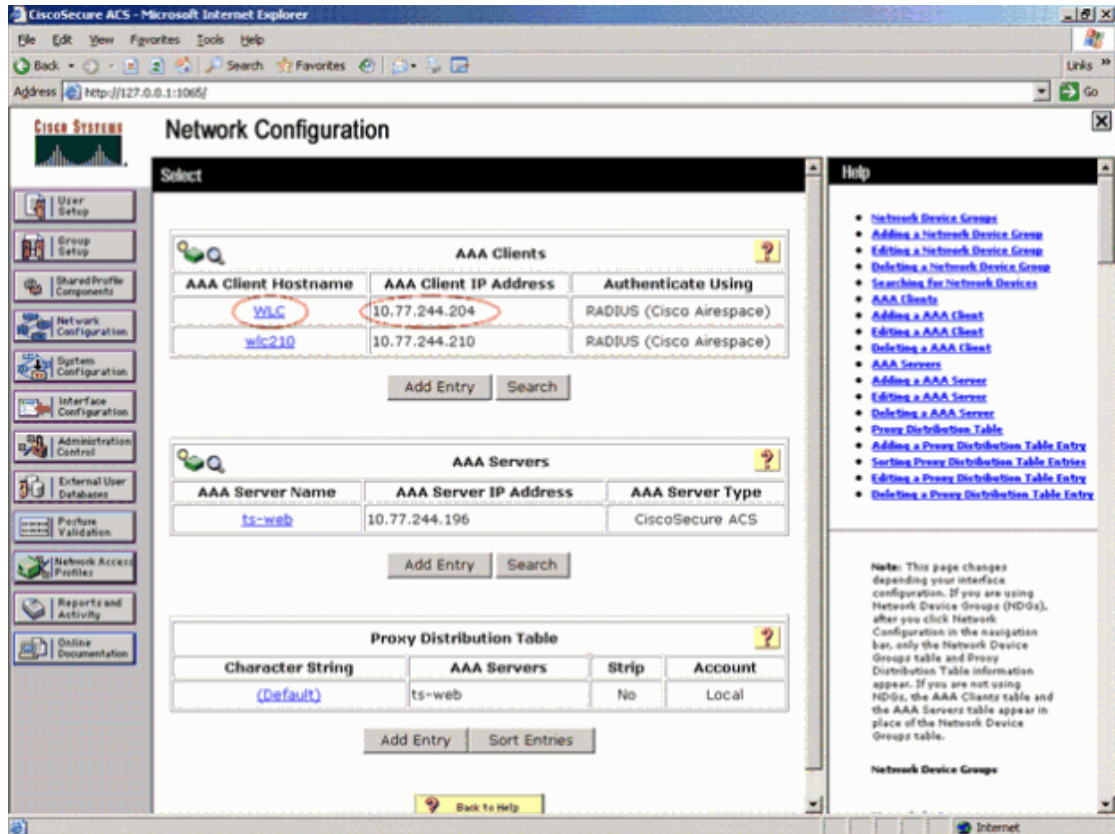


内部 Web 认证配置的核对及排障

核对 ACS 配置

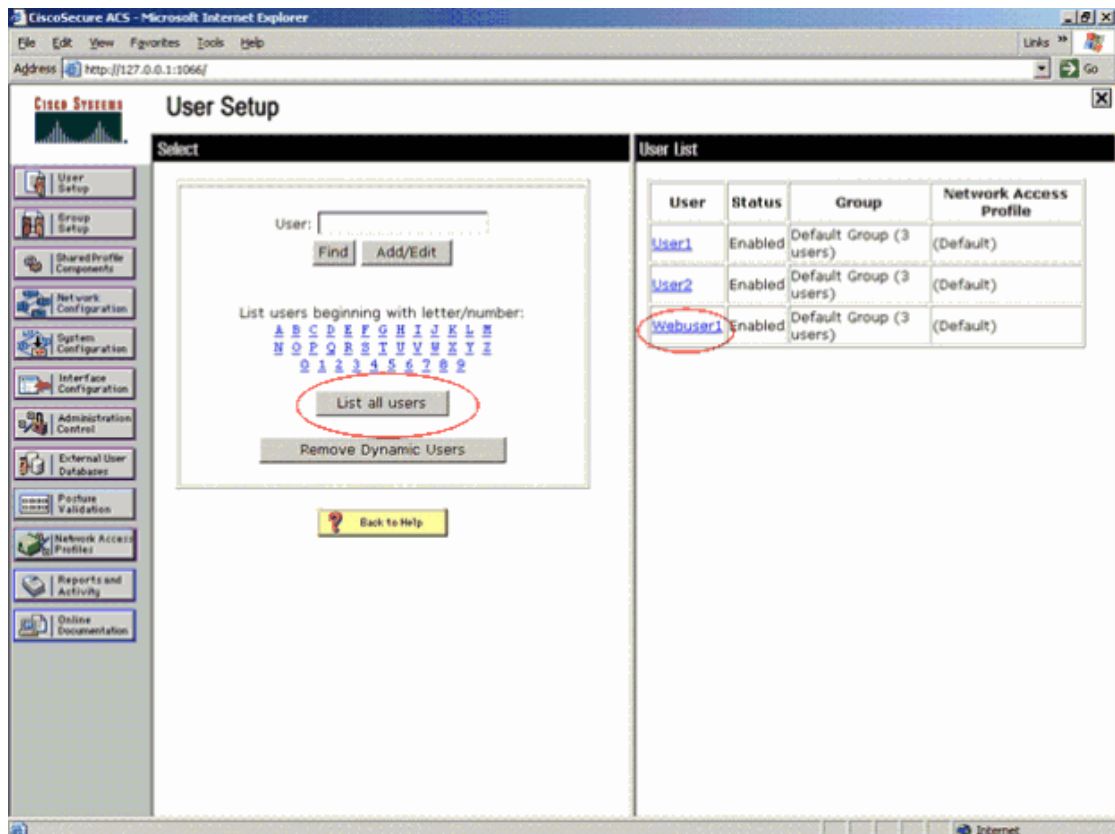
当你建立ACS时，记住要下载所有的补丁及最新的软件。这样会解决一些发生过的问题。在你使用Radius认证的时候，确保WLC配置成AAA客户端，如图19所示。点击左手边的**Network Configuration**菜单，进行检查。点击AAA客户端，核对密码及认证方式。更多关于如何配置AAA客户端的信息，参见思科ACS4.3用户手册的配置AAA客户端章节。

图 19



当你选择建立用户时，核对你是否确实建立了用户。点击**List All Users**。如图20所示，会出现一个窗口。确保所创建的用户在这个列表中。

图 20



核对内部 Web 认证配置

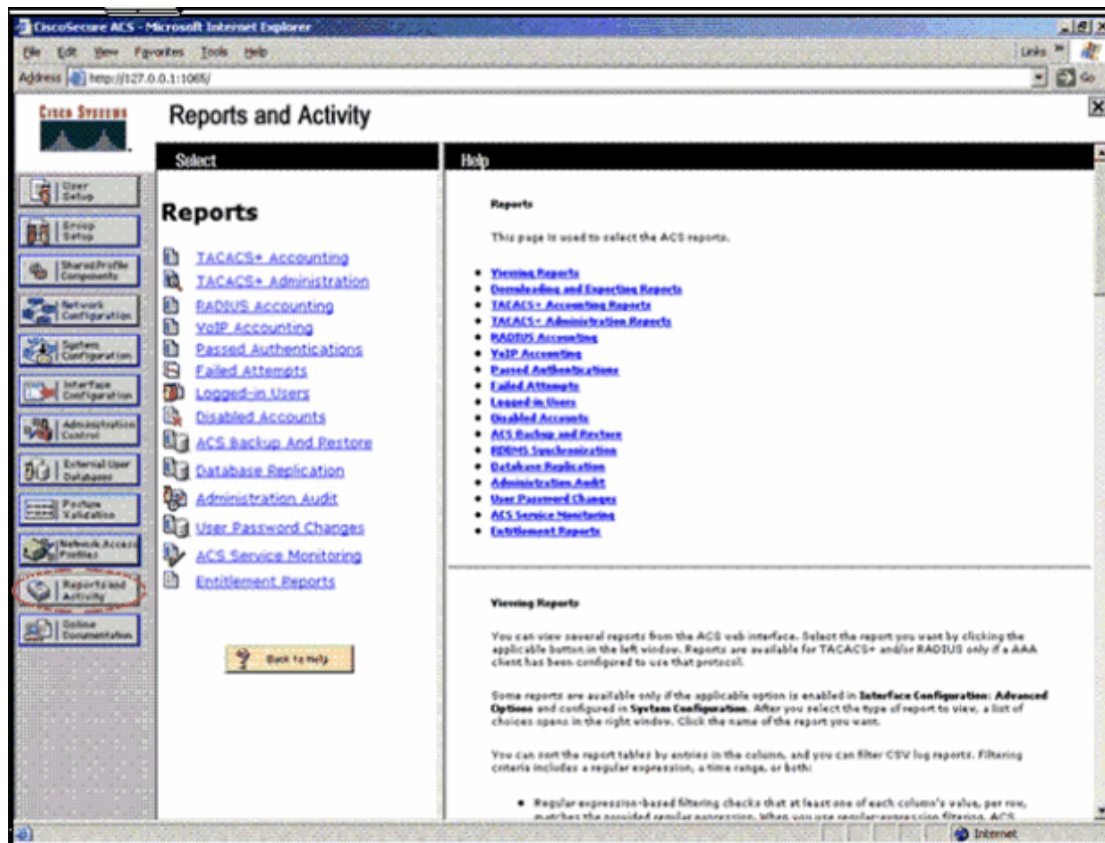
下文介绍如何检查内部web认证的配置是否工作正常。

Web认证的配置相对较为简单。牢记要在你的客户端上的无线连接检查配置属性。在无线网络栏下，检查**Use Windows to Configure My Wireless Network**配置。如果你使用的是Windows零配置方式，确保这个选项是勾选的。如果你使用的是其它的客户端，请参见相关的配置文档。确保virtual接口在**Controller > Interfaces**页面上配置正确。同时，检查WLAN/SSID配置，确保你激活了这个WLAN/SSID并且正确配置了web方式认证。

ACS 排障

如果你有密码认证的问题，点击ACS左下方的**Reports and Activity**，打开所有报告。在你打开了报告窗口后，你可以选择打开**RADIUS Accounting**，**Failed Attempts for login**，**Passed Authentications**，**Logged-in Users**，以及其他报告。这些报告是.csv文件格式的，你可以在本地打开这些文件。看图21。报告帮助发现认证的问题所在，比如错误的用户名密码。ACS 同样支持在线的文档。如果你没有接入工作着的网络，或者没有定义服务端口，ACS用使用你的以太端口的IP地址作为你的服务端口。如果你没有网络连接，你很有可能获得Windows的默认地址，类似169.254.x.x。

图 21



注意:如果你键入了任意的外部URL, WLC自动的将你转到内部的web认证页面。如果自动的重定向不工作, 你可以输入WLC的管理地址进行排障。查看浏览器的顶部的消息是否显示重定向到web认证。

内部 Web 认证排障

为了在你的PC上对无线连接进行排障, 带上思科Aironet 350无线网卡。某些早期的PC机带有不合规范的无线适配器。确保带有一块可信的网卡。记住这个网络配置是用在访客接入的环境下的。牢记数据流是明文的。唯一的安全措施是在web认证时候使用的用户名及密码。

Web认证经常被提及的一个问题就是页面重定向出现问题。完成以下检查:

1. 在WLC的版本早于3.2.150.10时, 用户必须手工键入<https://1.1.1.1/login.html>来连接web认证的窗口。但如果这样的问题发生在3.2.150.10以后的版本, 这就和DNS解析有关。当一个该SSID下的用户连接Internet的时候, 控制器的管理地址会做一个DNS询问, 查看这个URL是否合法。如果合法, 就会出现带有虚拟接口地址的认证页面。在用户成功登录之后, 原来的请求就会允许送回给客户端。因此, 确认DNS服务器是否正确配置。你可以通过**nslookup** 命令来查看DNS是否工作正常。更多信息, 参见思科bug号CSCsc68105 (限注册用户)。
2. 有时候是因为客户端的计算机安装了防火墙, 阻挡了Web认证页面。在你尝试连接登录页面前, 关闭防火墙。当web认证完成之后可以再打开防火墙。

3. 另外一个web认证不工作的原因是客户端的IP地址。确认客户端获得的地址是合法地址段内的。
4. 在使用访客接入时，在客户端浏览器上关闭代理设置。

注意：当WLC重定向用户去进行web认证时，你可以使用域名解析代替虚拟IP地址。你需要配置DNS名字并且在DNS上注册。这个配置是在控制器的虚拟接口下做的。你可以看见一个填写DNS的区域。完成这个配置后，重定向显示的是域名而不是1.1.1.1。

在 WLAN 上没有配置认证服务器时 Web 认证依然向外部认证服务器发送认证请求

这个问题发生在WLAN上配置的是web认证使用本地认证，同时配置了一个默认网络RADIUS服务器。如果客户端web认证失败，同时控制器上配置了外部的认证服务器，web认证就会把凭证发到外部认证服务器去确认。这个是由于思科bug号CSCsh35098（限注册用户）。解决的方法是将web RADIUS认证的方法从PAP改到CHAP（Controller – General）。通过这个改变，活动的数据库将拒绝认证。默认配置下，AD只使用PAP，无法理解CHAP的hash过的密码。

微软 IE 因为缓存重定向到 Web 认证登录页面

当用户使用Web认证，并且输入了用户名和密码成功登录后，浏览器会把用户重定向到登录页面而不是提供网络接入。

下面是实践发生的顺序：

1. 用户选择一个WLAN并且通过认证（获得IP地址）。
2. 用户打开了指向他们主页的web浏览器。
3. 浏览器自动重定向到虚拟接口地址（1.1.1.1）。
4. 虚拟接口地址拥有Web认证的登录页面，页面会要求一个 e-mail地址(或者用户名/密码)。
5. 用户输入自己的信息。
6. 虚拟接口重定向到一个特定的web页面。
7. 用户点击首页键，页面再次重定向到虚拟接口地址，再次要求输入登录信息。不过这次输入完之后没有重定向（一次又一次显示登录页面）。

这个是由于思科bug 号CSCse90894(限注册用户)造成的。你可以下载定制Web认证页面或者升级软件到4.0.206.0或者以后版本来解决这个问题。

下面是定制 HTML 的例子：

```
<html>
<head>
<title>Web Authentication</title>
<meta http-equiv="Pragma" content="no-cache">
```

```

</head>
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<title>Web Authentication</title>
<script>
function submitAction(){
    var link = document.location.href;
    var searchString = "redirect=";
    var equalIndex = link.indexOf(searchString);
    var redirectUrl = "";
    var urlStr = "";
    if(equalIndex > 0) {
        equalIndex += searchString.length;
        urlStr = link.substring(equalIndex);
        if(urlStr.length > 0){
            redirectUrl += urlStr;
            if(redirectUrl.length > 255)
                redirectUrl = redirectUrl.substring(0,255);
            document.forms[0].redirect_url.value = redirectUrl;
        }
    }
    document.forms[0].buttonClicked.value = 4;
    document.forms[0].submit();
}

function loadAction(){
    var url = window.location.href;
    var args = new Object();
    var query = location.search.substring(1);
    var pairs = query.split("&");
    for(var i=0;i<pairs.length;i++){
        var pos = pairs[i].indexOf('=');
        if(pos == -1) continue;
        var argname = pairs[i].substring(0,pos);
        var value = pairs[i].substring(pos+1);
        args[argname] = unescape(value);
    }
    //alert( "AP MAC Address is " + args.ap_mac);
    //alert( "The Switch URL is " + args.switch_url);
    document.forms[0].action = args.switch_url;
    // This is the status code returned from webauth login action
    // Any value of status code from 1 to 5 is error condition and user should be shown error as
below or
    //modify the message as it suits the customer
    if(args.statusCode == 1){
        alert("You are already logged in. No further action is required on your part.");
    }
}

```



```
</div>
</form>
</body>
<head>
<META HTTP-EQUIV="Pragma" CONTENT="no-cache">
</HEAD>
</html>
```

定制 Web 认证页面原则

当你创建定制的 Web 认证登录页面时，使用以下原则：

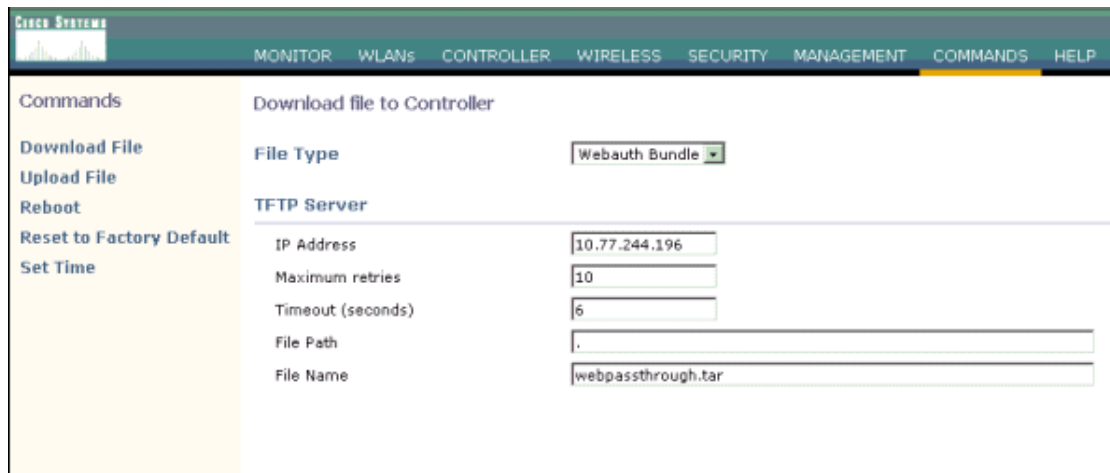
- 登录页面命名为**login.html**。控制器通过名字提供web认证URL。当控制器解压了认证页面后没有找到这个文件，会出现一个错误信息。
- 包含输入用户名和密码的区域。
- 保存重定向URL作为原始URL的隐藏输入
- 解压并在原始URL页面上实际的URL。
- 包含解码返回状态代码的脚本。
- 确保所有主页上使用的路径（例如，指向图片）是关联的。
- 在你上载定制页面到控制器之前，将页面及图片以.tar格式压缩。当这个.tar 文件通过TFTP服务器下载后，WLC将把它解压以非压缩的形式保存在文件系统中。如果你加载了一个非GNU兼容的.tar文件的包，控制器无法解压，会出现如下错误信息：**Extracting error**和**TFTP transfer failed**。因此思科推荐你使用一个GNU兼容的应用，例如PicoZip 来解压.tar 文件。

定制 Web 认证成功或者 Web 认证登录页面

在 WLC 上定制 Web 认证成功或者 Web 认证登录页面

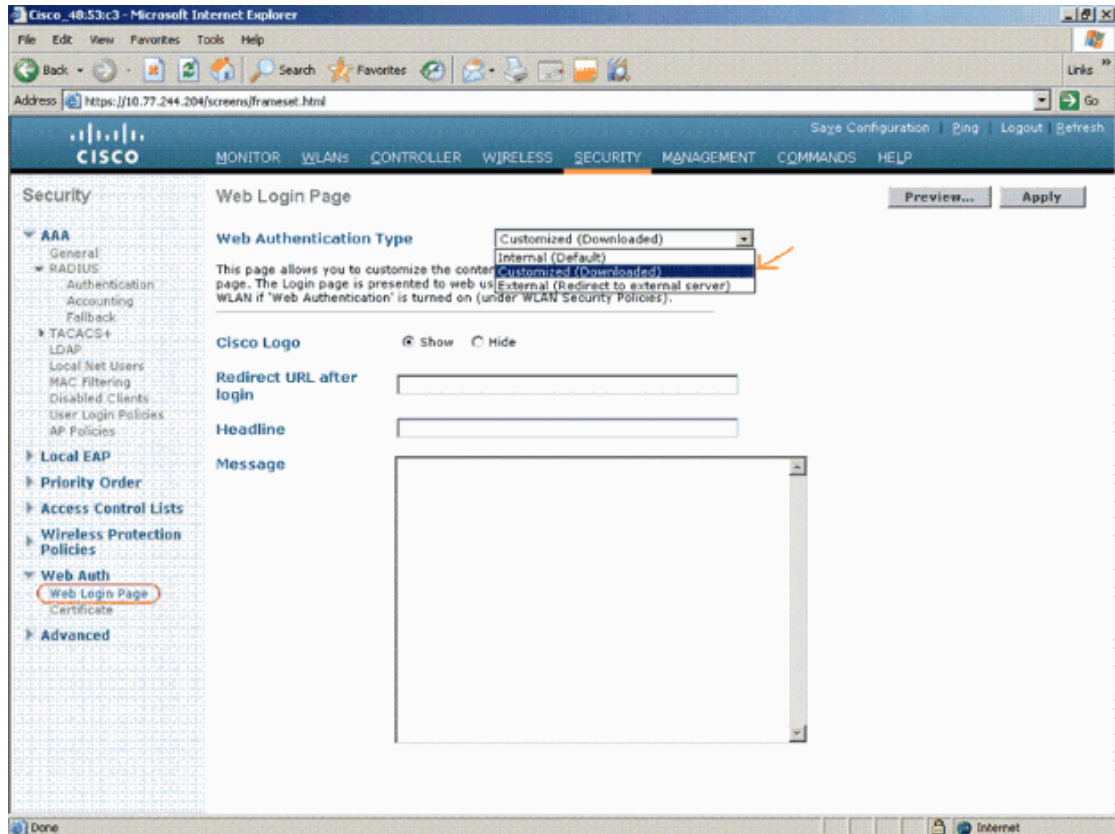
通过以下步骤，在 WLC 的 GUI 上定制 Web 认证成功或者 Web 认证登录页面：

1. 在 WLC 的 GUI 上，选择 **Commands > Download File**。
将文件上载到 WLC 的页面出现了。
2. 通过 File Type 的下拉菜单，选择 **Webauth Bundle**。
3. 输入 TFTP 服务器的地址，文件路径 (TFTP 服务器的根目录) 和定制的登录脚本的文件名称 (需要下载的 .tar 文件的名字)。点击 **Download**。
新的定制的登录页面下载完毕。以下是一个例子：



Download file to Controller	
File Type	Webauth Bundle
TFTP Server	
IP Address	10.77.244.196
Maximum retries	10
Timeout (seconds)	6
File Path	.
File Name	webpassthrough.tar

4. 选择 **Security > Web Login Page**，进入 Web 登录页面。
5. 通过 Web Authentication Type 下拉框，选择 **Customized (Downloaded)**。
6. 点击 **Apply**，保存变更。下图显示了如何完成该步骤。



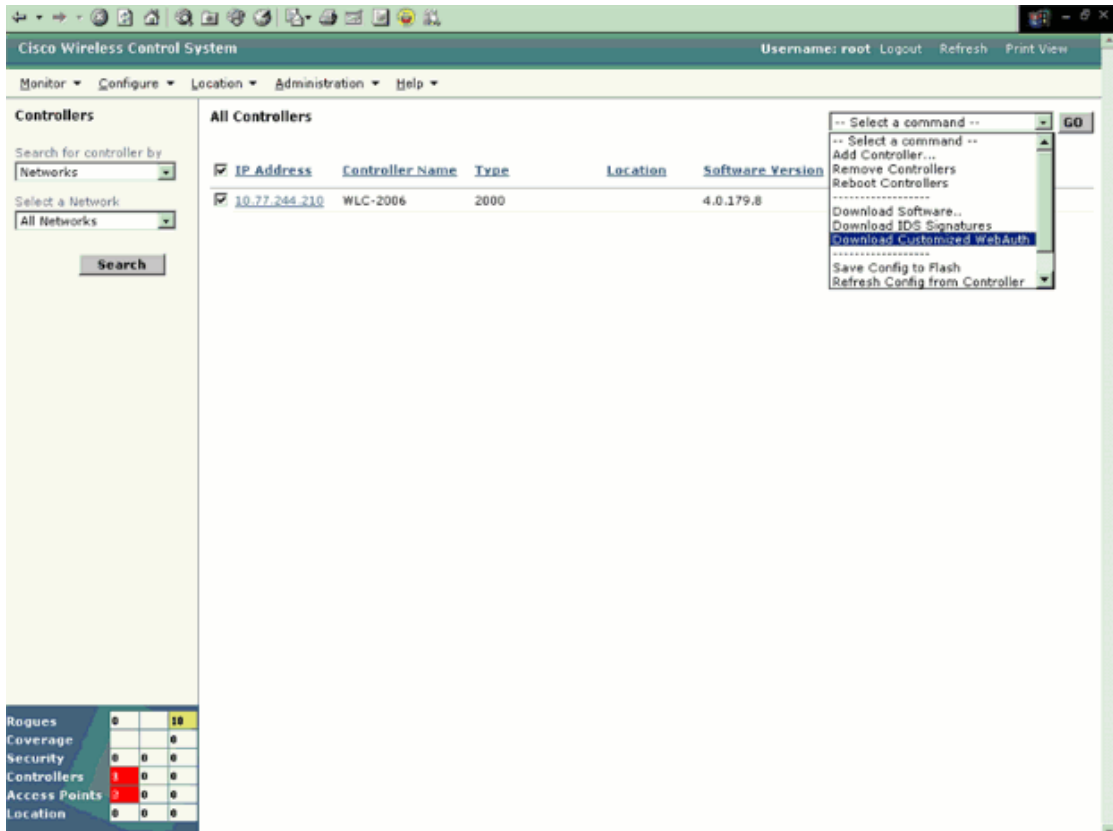
7. 保存控制器配置。

注意：在控制器软件版本4.1之前，一台WLC只能有一个web认证的页面。更多信息，参见思科无线局域网控制器配置手册，5.0版本的在WLAN上使用GUI分配登录，登录失败，和登出页面的章节。

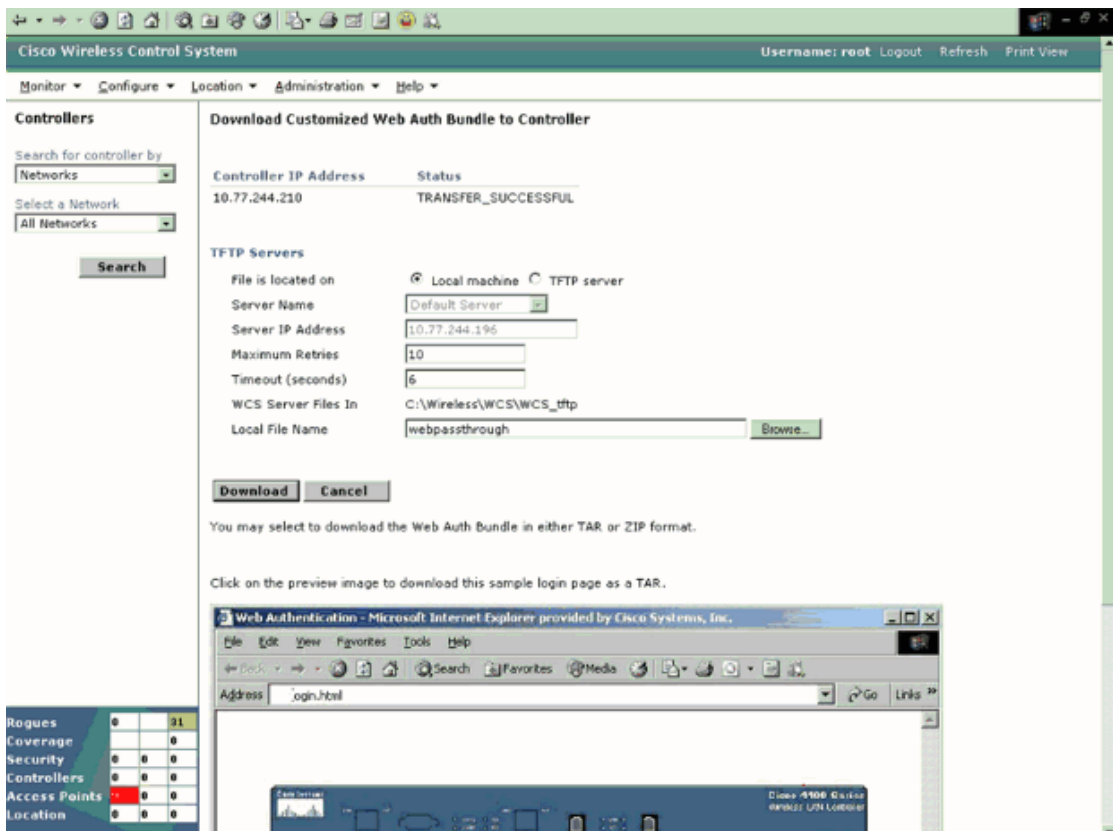
在 WCS 上定制 Web 认证成功或者 Web 认证登录页面

通过以下步骤，完成在WCS上定制Web通过或者Web认证登录页面。

1. 通过WCS的GUI，选择**Configure > Controllers**。
页面会显示所有的控制器。
2. 选择需要定制Web通过或者Web认证登录页面的控制器。
3. 在Command 下拉菜单里，选择**Download Customized WebAuth**，点击Go。



4. 在控制器的Download Customized Web Auth Bundle页面，键入文件名字(定制的.tar文件的名字)点击**Download**。
5. 定制的Web认证/Web认证成功页面就推给了控制器。



6. 完成在 WLC 上定制 Web 认证成功或者 Web 认证登录页面部分中的第 4 到第 7 步。

在 WLAN 上分配登录，登录失败，登出页面

你可以在每个 WLAN 上显示不同的 web 认证的登录，登录失败以及登出的页面。这个特性允许显示基于用户的不同的认证页面，例如某个公司的不同部门的访客或者雇员。不同的认证页面特性支持所有的 web 认证（内部，外部，定制）。尽管如此，不同的认证失败及登出页面只有在你选择定制的 web 认证方式时才可用。

使用 GUI 分配 WLAN 的登录，登录失败和登出页面

你可以通过控制器的 GUI 分配 WLAN 的 web 认证登录，登录失败和登出页面。

完成以后步骤：

1. 点击 WLANs，打开 WLAN 页面。
2. 点击想要分配 Web 登录，登录失败和登出页面的 WLAN 的 profile 的名字。
3. 选择 **Security > Layer 3**。
4. 确认选择了 **Web Policy** 和 **Authentication**。
5. 为了重载全局 web 认证页面，勾选 **Override Global Config** 框。
6. 当 Web Auth Type 下拉框出现时，选择以下几个选项来定义无线访客的 web 认证页面类型：
 - ◆ **Internal** 显示默认的 web 登录页面。这个是默认配置。
 - ◆ **Customized** 显示定制的 web 认证登录，登录失败和登出页面。如果你选择这个选项，会出现三个独立的下拉框，分别为登录，登录失败和登出页面的选择框。你不必为三个选项都选择定制的面。如果你不想显示一个定制的面，在下拉菜单中选择 **None**。
注意：这些可选的登录，登录失败和登出页面是作为 webauth.tar 文件下载到控制器的。关于下载定制页面，参见下载定制 Web 认证登录页面。
 - ◆ **External** 重定向用户到外部的服务去认证。如果使用该选项，你需要在 URL 栏输入外部服务器的 URL。
你可以在 WLANs > Edit (Security > AAA Servers) 页面上，选择特定的 RADIUS 或者 LDAP 服务器来提供外部认证。此外，你可以定义这些服务器的优先级。
7. 如果你在第 6 步中选择 External 作为 web 认证的方式，点击 AAA Servers，在下拉框中选择最多三个 RADIUS 或者 LDAP 服务器。
注意：RADIUS 和 LDAP 外部服务器需要已在 WLC 上配置，这样可以在 WLANs > Edit (Security > AAA Servers) 页面上选择。你可以在 RADIUS Authentication Servers 页面和 LDAP Servers 页面上配置这些服务器。
8. 为了配置这些用于 web 认证的服务器的优先级，完成以下步骤。默认的顺序是 local, RADIUS, LDAP。
 - a) 在上和下按钮边上的区域中，高亮选择你想用来最先认证的服务器类型 (local, RADIUS, or LDAP) 。
 - b) 点击 **Up** 和 **Down** 按钮，直到你想要的类型出现在区域的最上面。
 - c) 点击 < 箭头，将服务器类型移到左边的区域。
 - d) 重复上述步骤，完成其他服务器优先级的分配。
9. 点击 **Apply**，发送配置变更。
10. 点击 **Save Configuration**，保存配置。

基于 802.1x 认证的有条件的 Web 重定向

这是一个控制器4.0.206.0版本以后的新特性，它允许用户在成功完成802.1x认证后有条件的重定向到特定的web页面。这样的条件包括当用户的密码到期时，当用户为继续使用付费，等等。你可以在RADIUS服务器上定义重定向页面以及发生重定向的条件。如果RADIUS服务器返回思科AV-pair "url-redirect"，接着用户打开浏览器是就被重定向到特定的URL。如果服务器也返回了思科AV-pair "url-redirect-acl"，特定的访问列表就会被当作认证前的访问控制列表被应用到这个客户端。这个客户端在这里不被认为是具有全部权限的，只能访问认证前的访问控制列表允许的数据。

在客户端在特定的URL完成了特定的操作(例如，修改了密码或者付了费用)，用户需要重新认证。当RADIUS服务器没有回复"url-redirect"，客户端认为是拥有全部权限的，他的数据流就可以通过。有条件的web重定向特性只适用于配置802.1x或者WPA1+WPA2作为2层安全策略的WLAN上。你可以通过控制器的GUI或者CLI配置这个特性。

关于这个特性的更多信息以及如何配置这个特性，请阅读4.0.206.0的发布信息，你可以在思科无线局域网控制器发布信息和轻型无线接入点发布信息中找到。

相关信息

- [Cisco Wireless LAN](#)
- [Wired Guest Access using Cisco WLAN Controllers Configuration Example](#)
- [Cisco Wireless LAN Controller Configuration Guide, Release 5.0 – Managing User Accounts](#)
- [Authentication of Wireless LAN Controller's Lobby Administrator via RADIUS Server](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) |

[Trademarks of Cisco Systems, Inc.](#)

更新时间: 2008-10-13

文档编号: 69340
