无线局域网控制器 Web 身份验证配置示例

Contents

Introduction

本文档介绍思科如何实现 Web 身份验证以及如何配置思科 4400 系列无线 LAN (WLAN) 控制器 (WLC) 以支持内部 Web 身份验证。

Prerequisites

Requirements

本文档假设您已对 4400 WLC 进行了初始配置。

Components Used

本文档中的信息基于以下软件和硬件版本：

- 运行版本 7.0.116.0 的 4400 系列 WLC
- 安装在 Microsoft® Windows 2003 Server 上的思科安全访问控制服务器 (ACS) 版本 4.2

- Cisco Aironet 1131AG 系列轻量级无线接入点
- 运行版本 4.0 的 Cisco Aironet 802.11 a/b/g CardBus 无线适配器

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.

Web 身份验证

Web 身份验证是第三层安全功能，会导致控制器不允许接收来自特定客户端的 IP 数据流（DHCP 和 DNS 相关数据包除外），直到该客户端正确提供有效的用户名和密码。它是一种不需要请求者或客户端实用程序的简单身份验证方法。Web 身份验证通常由希望部署访客接入网络的客户使用。典型的部署可能包括如 T-Mobile 或 Starbuck 之类的“热点”位置。

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 身份验证可使用以下方法来执行：

- WLC 上的默认登录窗口
- WLC 上的默认登录窗口的修改版本
- 您在外部 Web 服务器上配置的自定义登录窗口（外部 Web 身份验证）
- 您下载到控制器的自定义登录窗口

在本文档中，为无线 LAN 控制器配置内部 Web 身份验证。

Web 身份验证过程

当用户连接到已配置 Web 身份验证的 WLAN 时，会进行身份验证：

- 用户打开 Web 浏览器并输入 URL，例如，http://www.cisco.com。客户端将发出该 URL 的 DNS 请求，以获取目标 IP。WLC 将 DNS 请求分流到 DNS 服务器，并且 DNS 服务器通过 DNS 回复作出响应，该回复包含目的地 www.cisco.com 的 IP 地址。这反过来又会转发给无线客户端。
- 然后，客户端尝试打开与目标 IP 地址之间的 TCP 连接，它会发出发往 www.cisco.com 的 IP 地址的 TCP SYN 数据包。
- WLC 已为客户端配置规则，因此可用作 www.cisco.com 的代理。它将 TCP SYN-ACK 数据包发回给客户端，将来源作为 www.cisco.com 的 IP 地址。客户端发回 TCP ACK 数据包，以完成三次 TCP 握手，从而完全建立 TCP 连接。
- 客户端发送发往 www.cisco.com 的 HTTP GET 数据包。WLC 拦截此数据包并发送以进行重定向处理。HTTP 应用程序网关准备 HTML 主体并将其作为客户端 HTTP GET 请求的应答返回。此 HTML 使客户端前往 WLC 的默认网页 URL，例如 http://<Virtual-Server-IP>/login.html。
- 客户端断开与 IP 地址（例如，www.cisco.com）的 TCP 连接。
- 现在客户端希望前往 http://1.1.1.1/login.html。因此，客户端会尝试使用 WLC 的虚拟 IP 地址打开 TCP 连接。它将 1.1.1.1 的 TCP SYN 数据包发送至 WLC。
- WLC 返回 TCP SYN-ACK，而客户端则发回 TCP ACK 至 WLC，以完成握手。

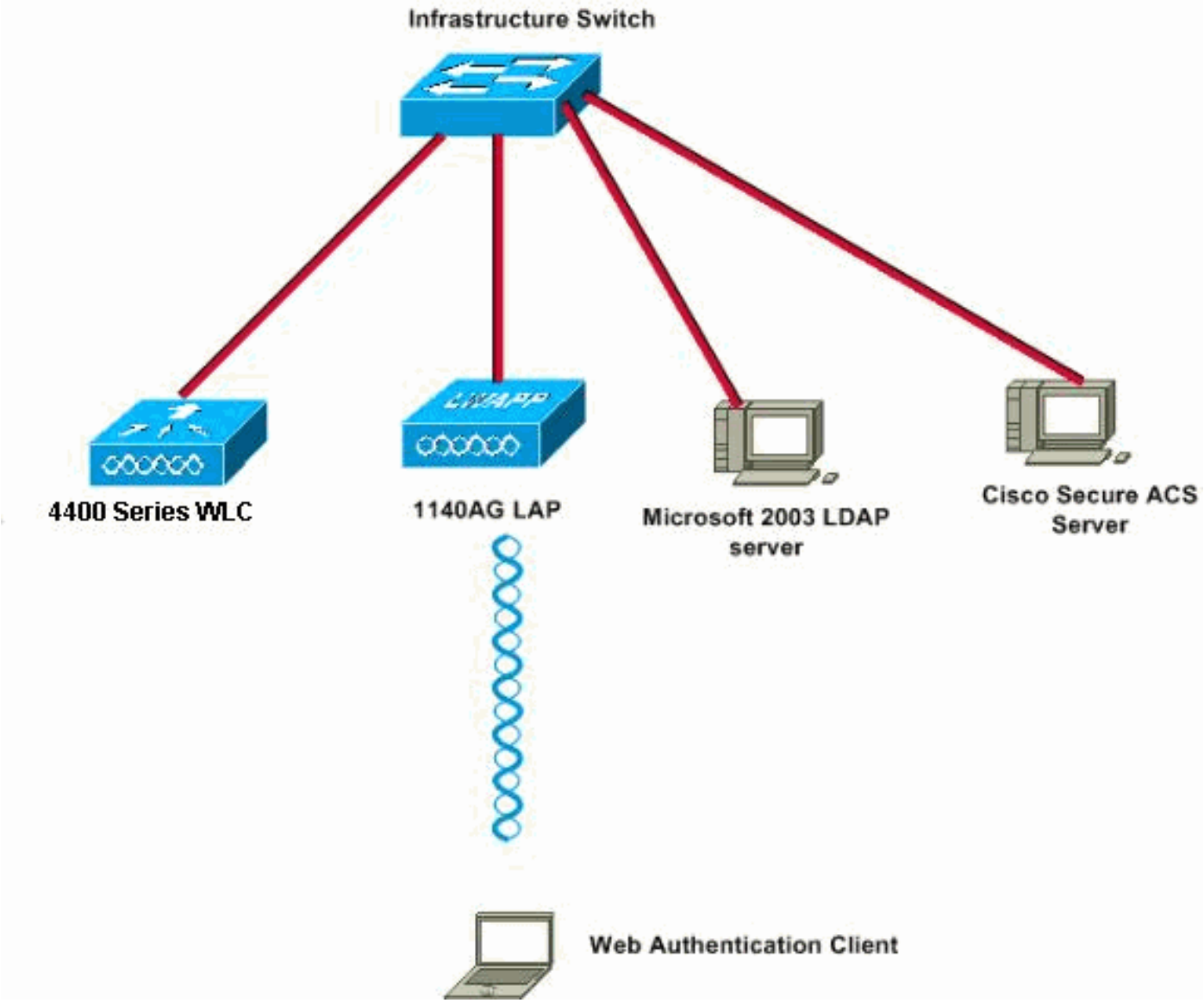
- 客户端会将 /login.html 的 HTTP GET 发送到目的地 1.1.1.1，以便请求登录页。
- 此请求由 WLC 的 Web 服务器确认允许，该服务器返回默认登录页。客户端将在浏览器窗口接收登录页，用户可以前往该窗口并登录。

以下是思科支持社区 视频的链接，该视频介绍了 Web 身份验证过程：

思科无线 LAN 控制器 (WLC) 上的 Web 身份验证

网络设置

本文档使用以下网络设置：



配置用于 Web 身份验证的控制器

在本文档中，为 Web 身份验证配置 WLAN 并映射到专用 VLAN。以下是配置用于 Web 身份验证的 WLAN 所包含的步骤：

- 创建 VLAN 接口
- 配置用于内部 Web 身份验证的 WLC
- 添加 WLAN 实例
- 配置身份验证类型（在 Web 身份验证中验证用户身份的三种方式）

本部分提供有关如何配置用于 Web 身份验证的控制器的信息。

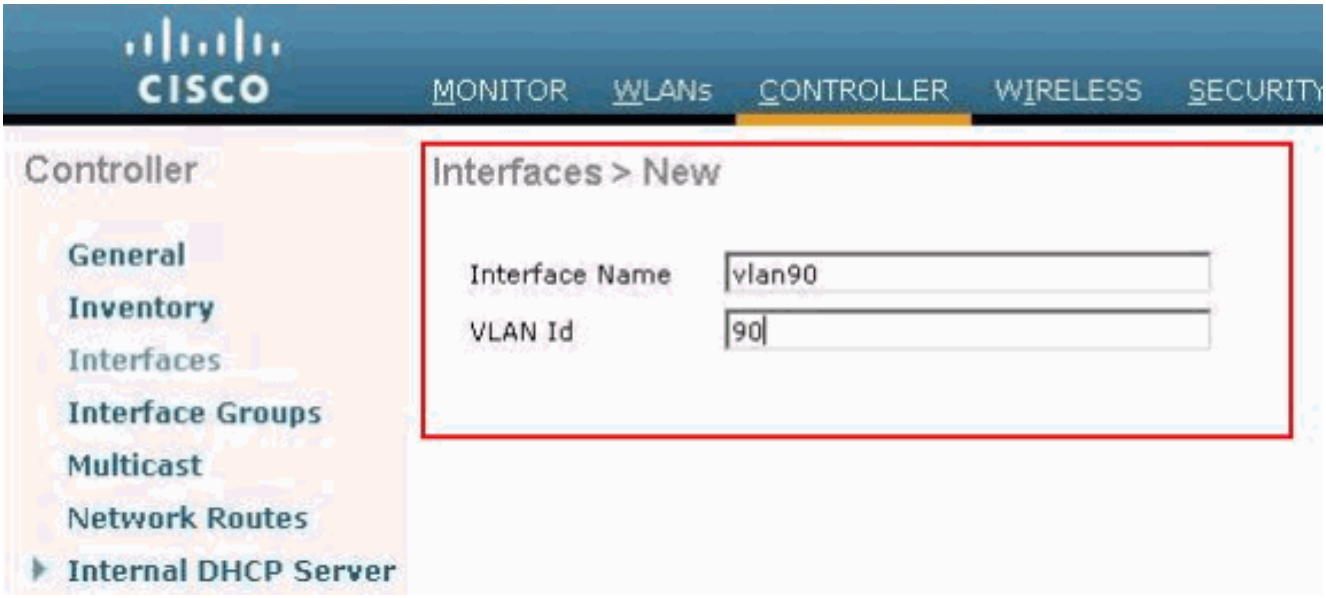
以下是本文档中使用的 IP 地址：

- WLC 的 IP 地址是 10.77.244.204。
- ACS 服务器的 IP 地址是 10.77.244.196。

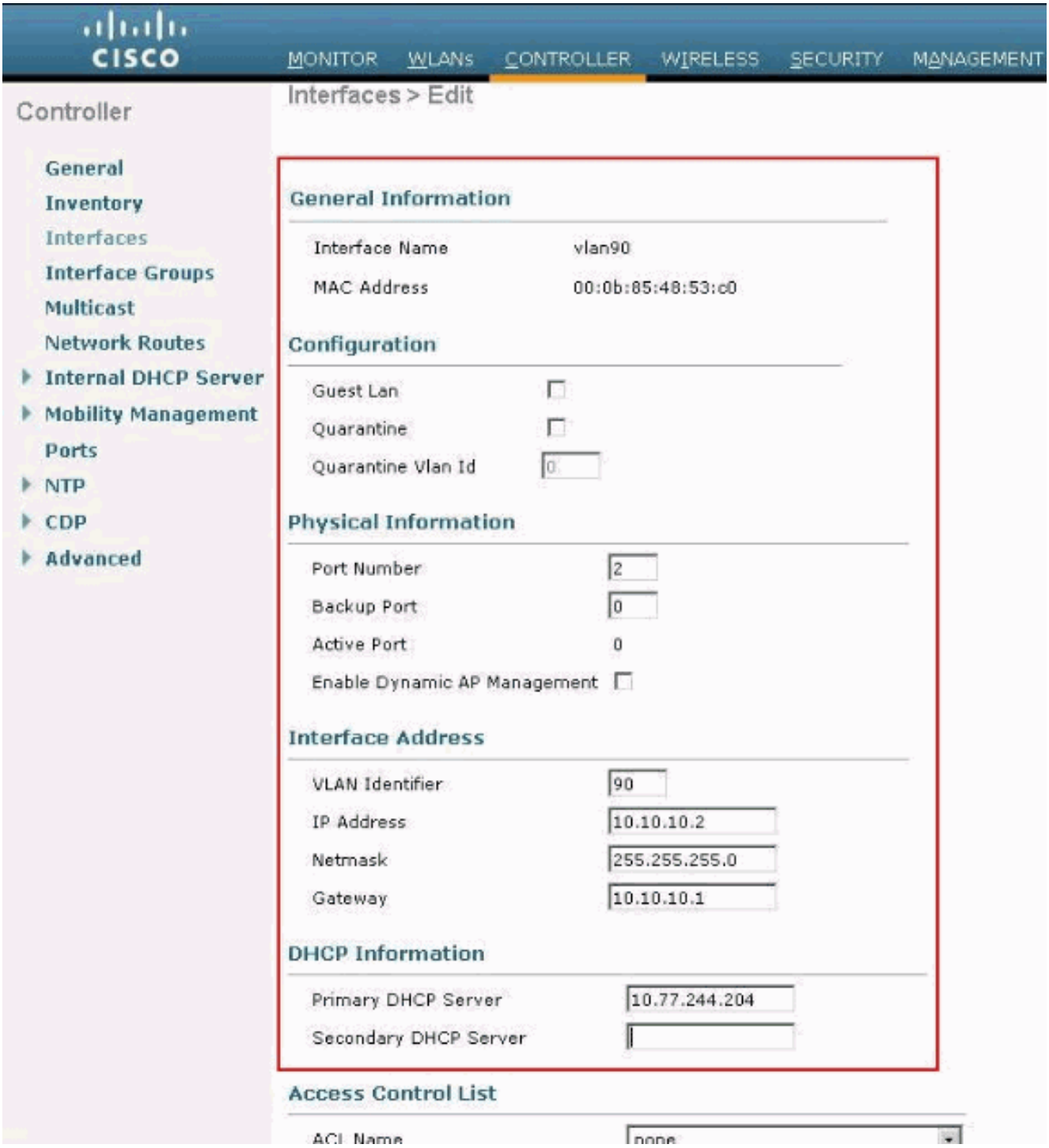
创建 VLAN 接口

完成这些步骤：

1. 在无线 LAN 控制器 GUI 中，从顶部的菜单中选择 **Controller**，从左侧的菜单中选择 **Interfaces**，然后点击窗口右上角的 **New** 以创建一个新的动态接口。此时会显示 **Interfaces > New** 窗口。本示例使用 VLAN ID 为 90 的接口名称 *vlan90*：



2. 单击 **Apply** 以创建 VLAN 接口。此时会显示 **Interfaces > Edit 窗口**，要求您填写接口特定信息。
3. 本文档使用以下参数：IP 地址 - 10.10.10.2子网掩码 - 255.255.255.0（24 位）网关 - 10.10.10.1端口号 - 2主 DHCP 服务器 - 10.77.244.204**Note:** 此参数应为您的 RADIUS 或 DHCP 服务器的 IP 地址。在本示例中，由于内部 DHCP 范围是在 WLC 上配置的，因此 WLC 的管理地址被用作 DHCP 服务器。辅助 DHCP 服务器 - 0.0.0.0**Note:** 本示例中没有辅助 DHCP 服务器，因此使用 0.0.0.0。如果您的配置中有辅助 DHCP 服务器，请在此字段中添加服务器 IP 地址。ACL 名称 - 无

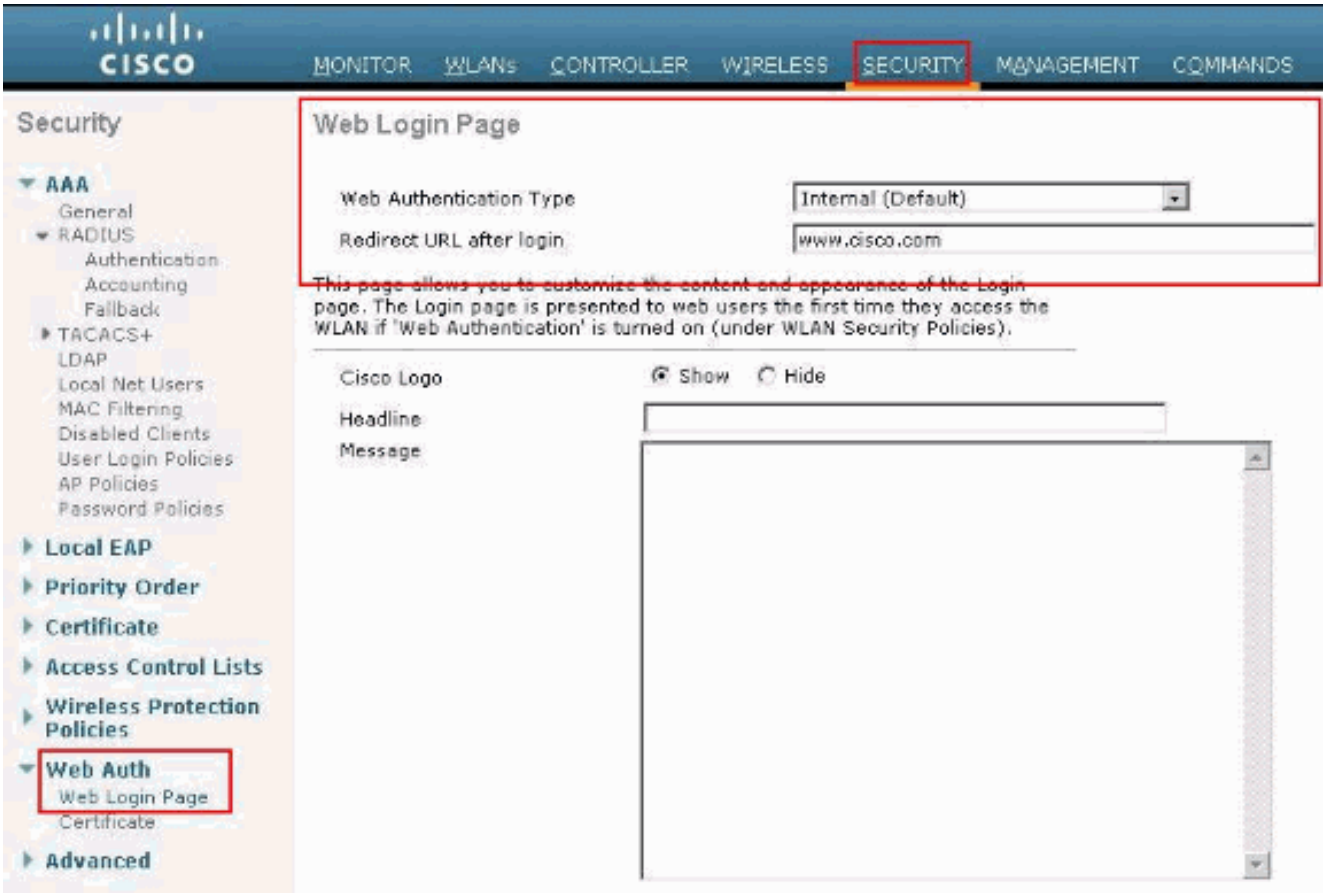


4. 单击 **Apply** 以保存更改。

配置用于内部 Web 身份验证的 WLC

下一步是配置用于内部 Web 身份验证的 WLC。内部 Web 身份验证是 WLC 上的默认 Web 身份验证类型。如果未更改此参数，则无需配置以启用内部 Web 身份验证。如果之前已更改 Web 身份验证参数，则请完成以下步骤，为内部 Web 身份验证配置 WLC：

1. 在控制器 GUI 中，依次选择 **Security> Web Auth > Web Login Page** 以访问 Web 登录页。
2. 在 Web Authentication Type 下拉框中，选择 **Internal Web Authentication**。
3. 在 **Redirect URL after login** 字段中，输入在身份验证成功之后终端用户将被重定向到的页面的 URL。



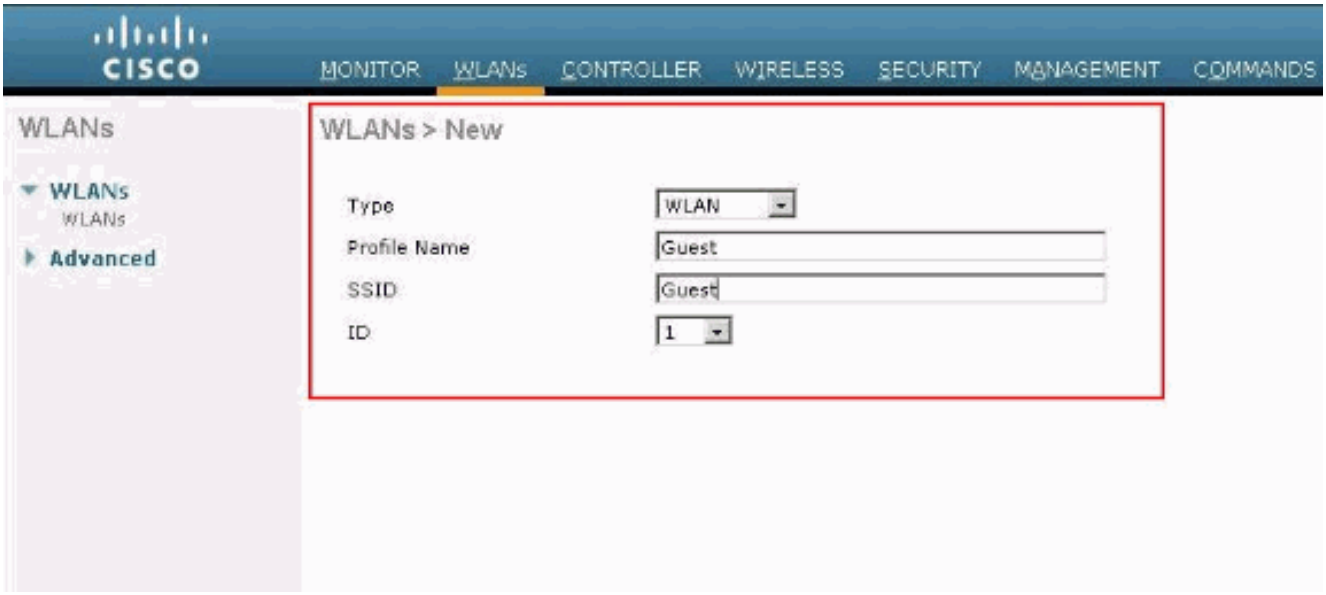
Note: 在 WLC 5.0 及以上版本中，也可自定义 Web 身份验证的注销页。有关如何进行配置的更多信息，请参阅无线局域网控制器配置指南的为每个 WLAN 分配登录、登录失败和注销页一节中的 5.2。

添加 WLAN 实例

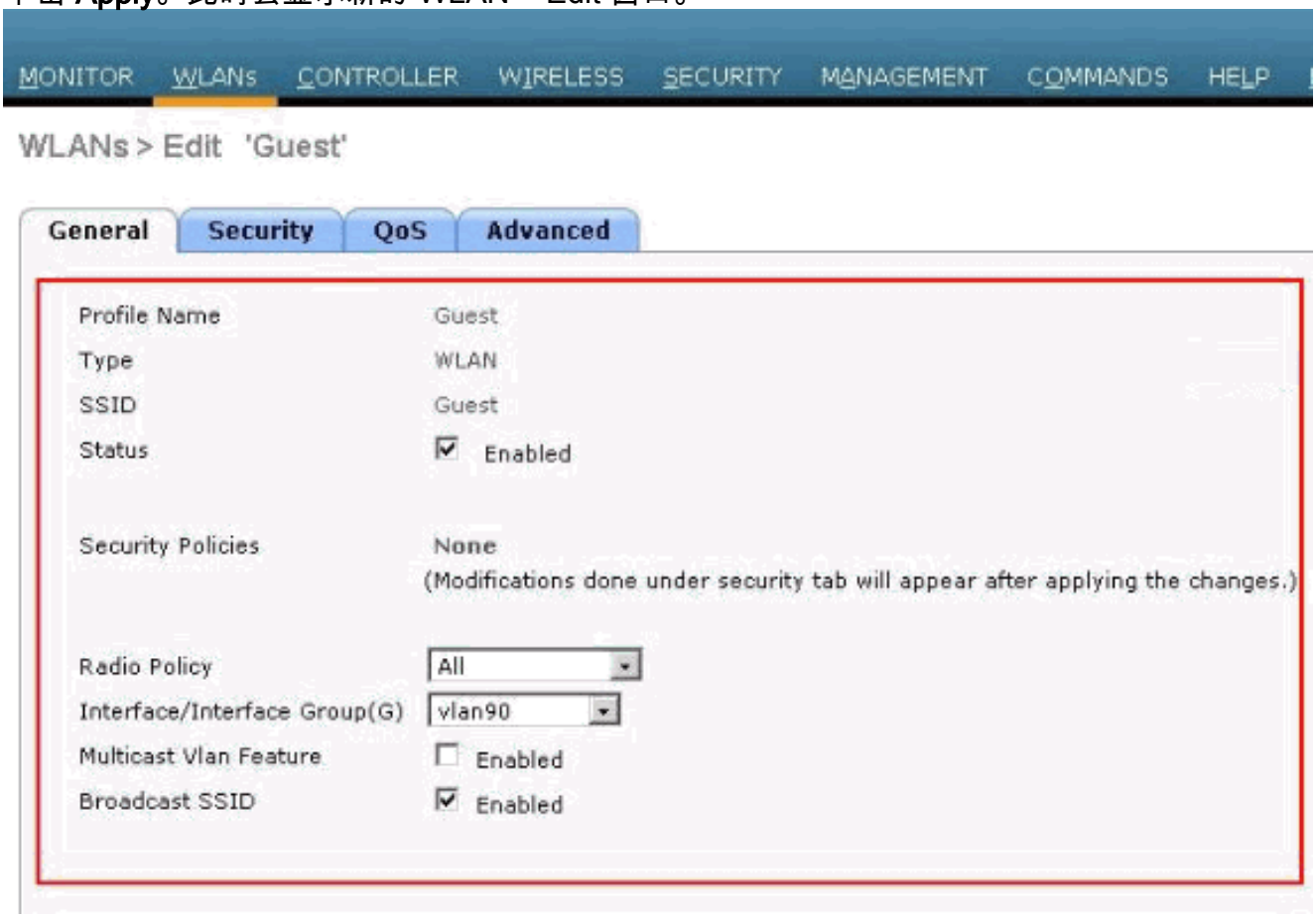
由于已启用内部 Web 身份验证且有一个专用于 Web 身份验证的 VLAN 接口，因此您必须提供一个新的 WLAN/SSID，以便为 Web 身份验证用户提供支持。

完成以下步骤以创建新的 WLAN/SSID：

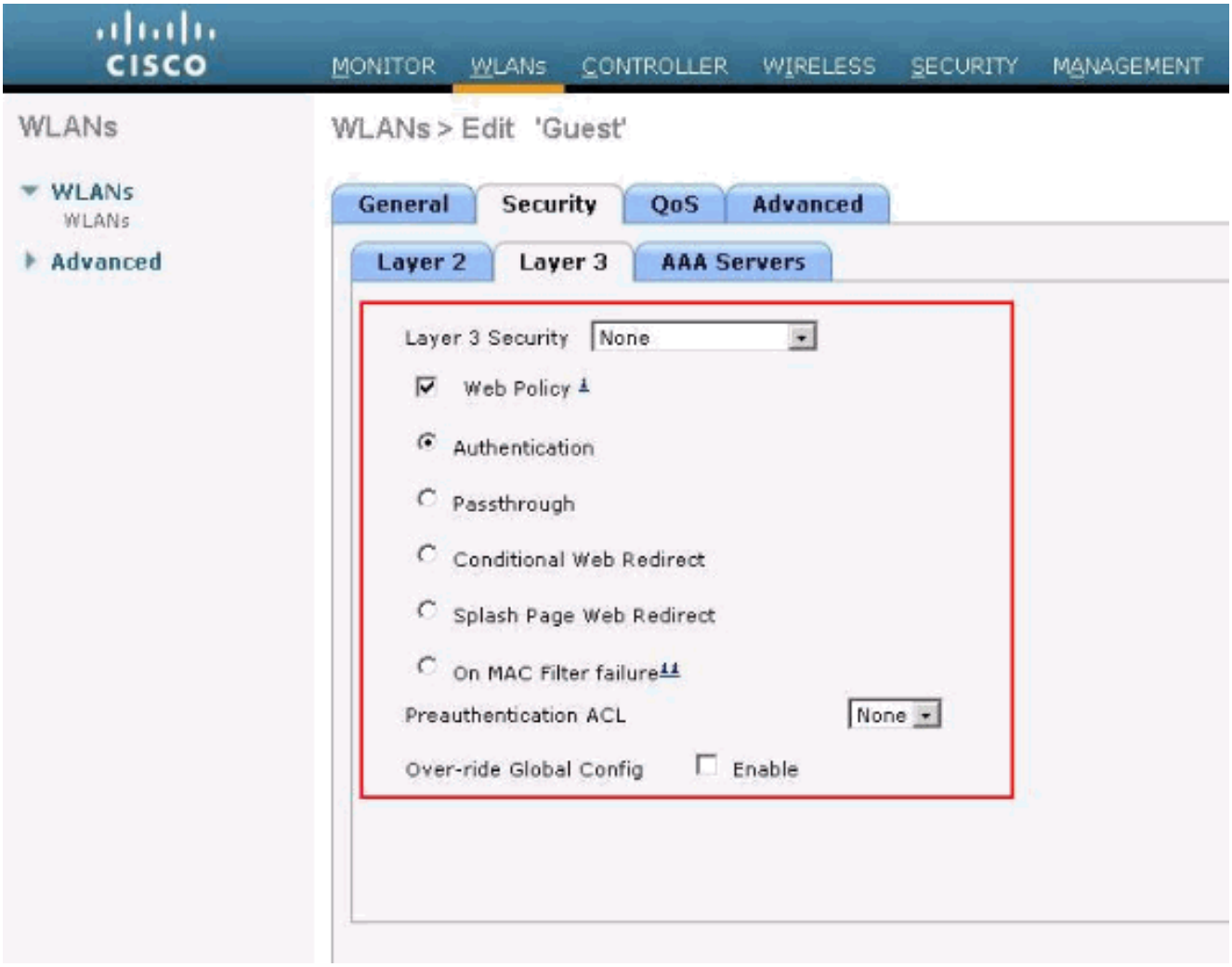
1. 在 WLC GUI 中，点击顶部菜单中的 **WLAN**，然后点击右上角的 **New**。选择 **WLAN** 作为“Type”。选择用于 Web 身份验证的配置文件名和 WLAN SSID。本示例对“Profile Name”和“WLAN SSID”都使用 **Guest**。



2. 单击 **Apply**。此时会显示新的 WLAN > Edit 窗口。



3. 选中 WLAN 的状态框以启用 WLAN。从“Interface”菜单中，选择您以前创建的 VLAN 接口的名称。在本示例中，接口名称为 *vlan90*。**Note:** 请保留此屏幕中其他参数的默认值。
4. 单击 **Security** 选项卡。完成以下步骤以配置 Web 身份验证：单击“Layer 2”选项卡并且将安全模式设置为 ***None***。**Note:** 您不能将 Web 穿透功能配置为使用 802.1x 的第 3 层安全，或将 WPA/WPA2 配置为 WLAN 的第 2 层安全。有关无线局域网控制器第 2 层和第 3 层安全兼容性的详细信息，请参阅无线局域网控制器第 2 层和第 3 层安全兼容性列表。单击“Layer 3”选项卡。选中 **Web Policy** 框并选择 ***Authentication 选项***，如下所示
：



单击“Apply”以保存 WLAN。此时将返回到“WLAN Summary”窗口。请确保 WLAN 表的“Security Policies”列下的“Web-Auth”对于 SSID 访客处于启用状态。

在 Web 身份验证中验证用户身份的三种方式

当您使用 Web 身份验证时，有三种方式验证用户身份。使用本地身份验证可在 Cisco WLC 中对用户进行身份验证。您也可以使用外部 RADIUS 服务器或 LDAP 服务器作为后端数据库来验证用户身份。

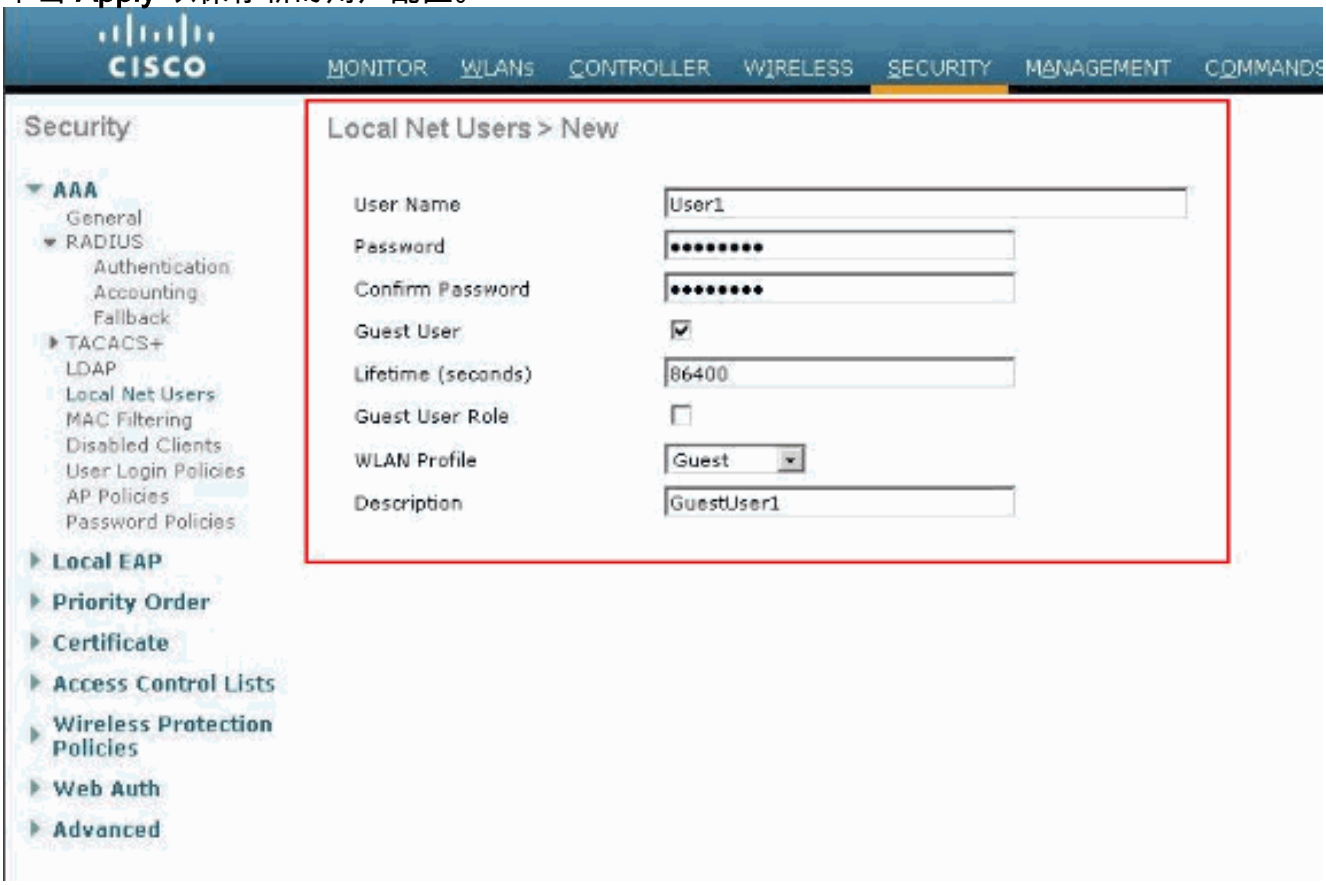
本文档为所有三种方法提供了一个示例配置。

本地 认证

访客用户的用户数据库存储在 WLC 的本地数据库中。WLC 根据此数据库对用户进行身份验证。

1. 从 WLC GUI 中，请选择 **Security**。
2. 在左侧的 AAA 菜单中单击 **Local Net Users**。

3. 单击 **New** 以创建一个新用户。此时将显示一个新窗口，要求提供用户名和口令信息。
4. 输入用户名和口令以创建新用户，然后确认要使用的口令。本示例创建名为 **User1** 的用户。
5. 如果需要，可添加说明。此示例使用 **Guest User1**。
6. 单击 **Apply** 以保存新的用户配置。



7. 重复步骤 3-6 以向数据库中添加更多用户。

用于 Web 身份验证的 RADIUS 服务器

本文档使用 Windows 2003 Server 上的无线 ACS 作为 RADIUS 服务器。您可以使用当前部署在网络中的任何可用的 RADIUS 服务器。

Note: 可以在 Windows NT 或 Windows 2000 Server 上设置 ACS。要从 Cisco.com 上下载 ACS，请参阅软件中心（下载）- Cisco 安全软件（仅限注册用户）。您需要 Cisco Web 帐户才能下载该软件。

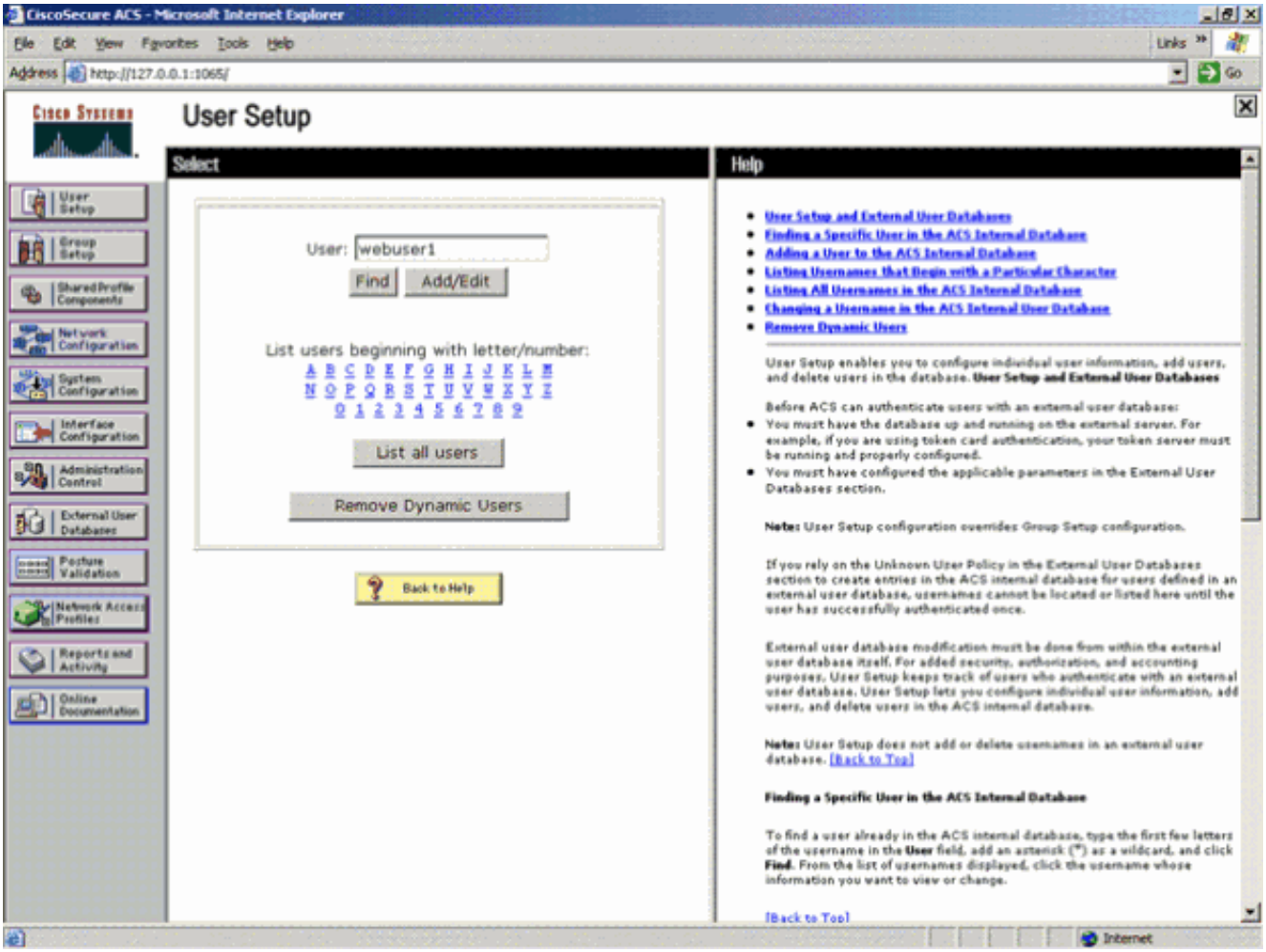
设置 ACS 部分说明了如何配置 RADIUS 的 ACS。您必须具有使用域名系统 (DNS) 和 RADIUS 服务器的全功能网络。

设置 ACS

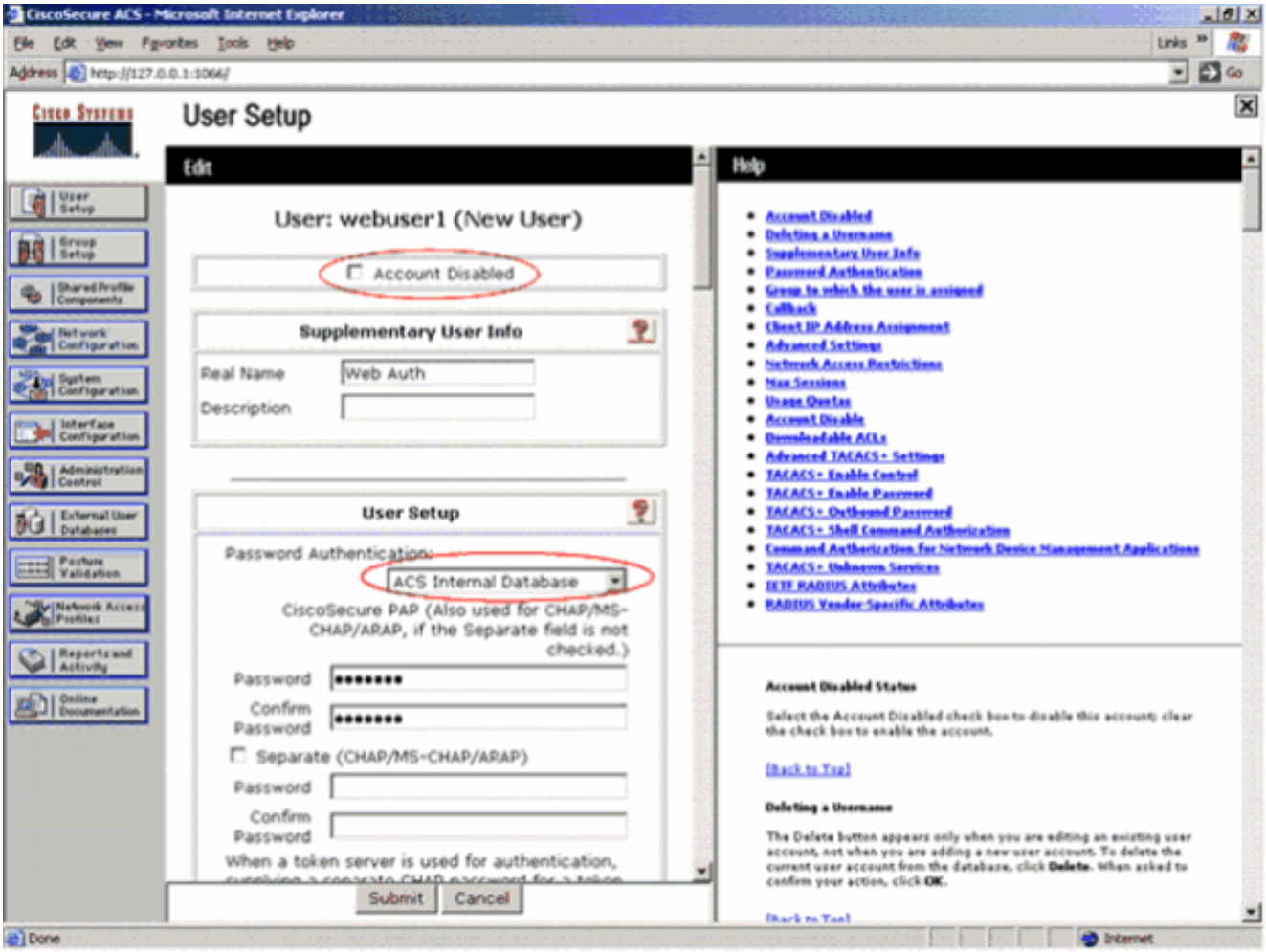
本部分提供有关如何设置 RADIUS 的 ACS 的信息。

在您的服务器上设置 ACS，然后完成以下步骤以创建进行身份验证的用户：

1. 当 ACS 询问您是否要在浏览器窗口中打开 ACS 以进行配置时，请单击 **Yes**。**Note:** 设置 ACS 之后，您的桌面上还会显示一个图标。
2. 在左侧的菜单中单击 **User Setup**。此操作会将您带往“User Setup”屏幕，如下所示：



3. 输入要用于 Web 身份验证的用户，然后单击 **Add/Edit**。在创建用户之后，第二个窗口打开，如下所示：

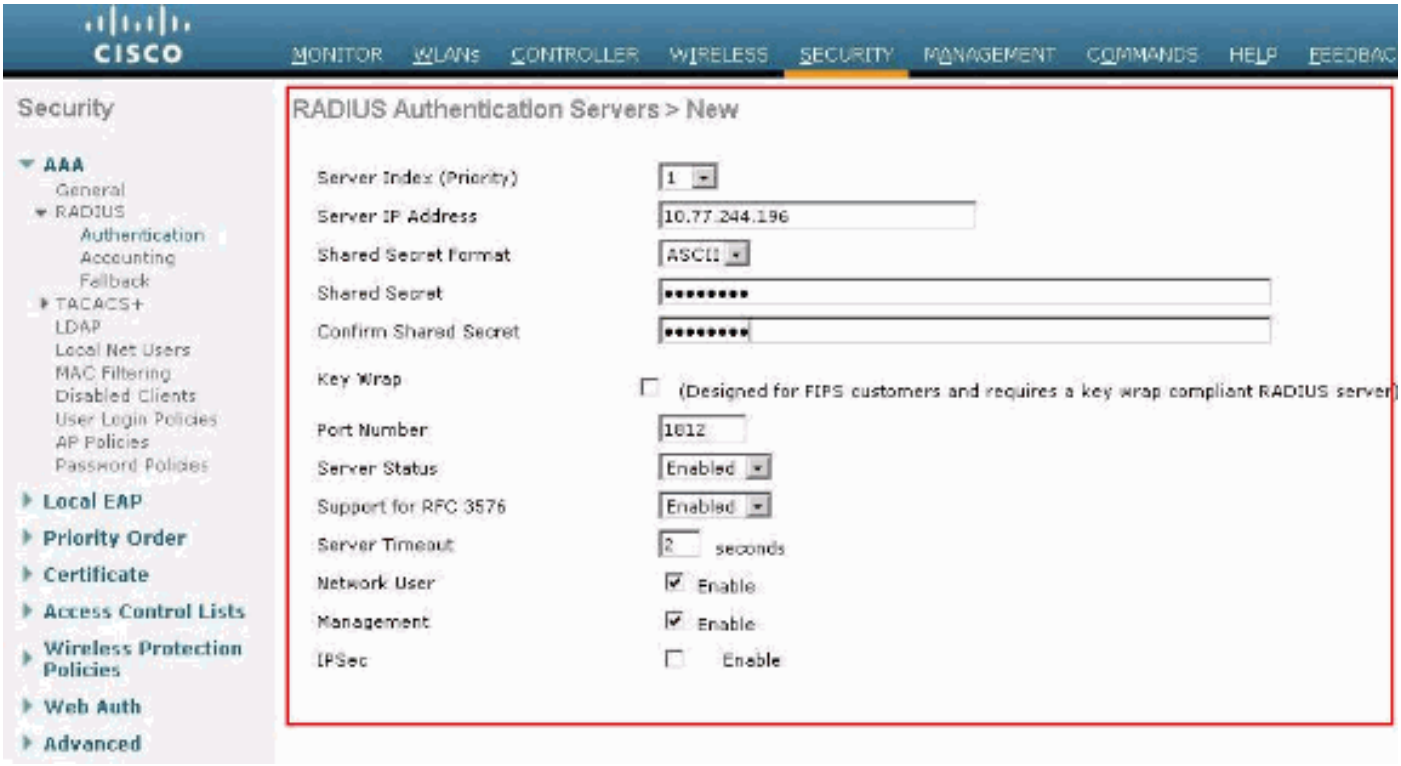


4. 确保未选中顶部的 **Account Disabled** 框。
5. 为“Password Authentication”选项选择 **ACSInternal Database**。
6. 输入密码。在 ACS 内部数据库中添加用户时，Admin 有一个选项可用于配置 PAP/CHAP 或 MD5-CHAP 身份验证。PAP 是控制器上的 Web 身份验证用户的默认身份验证类型。使用此 CLI 命令，Admin 可灵活地将身份验证方法更改为 chap/md5-chap：
   ```
   config custom-web radiusauth <auth method>
   ```
7. 单击 **submit**。

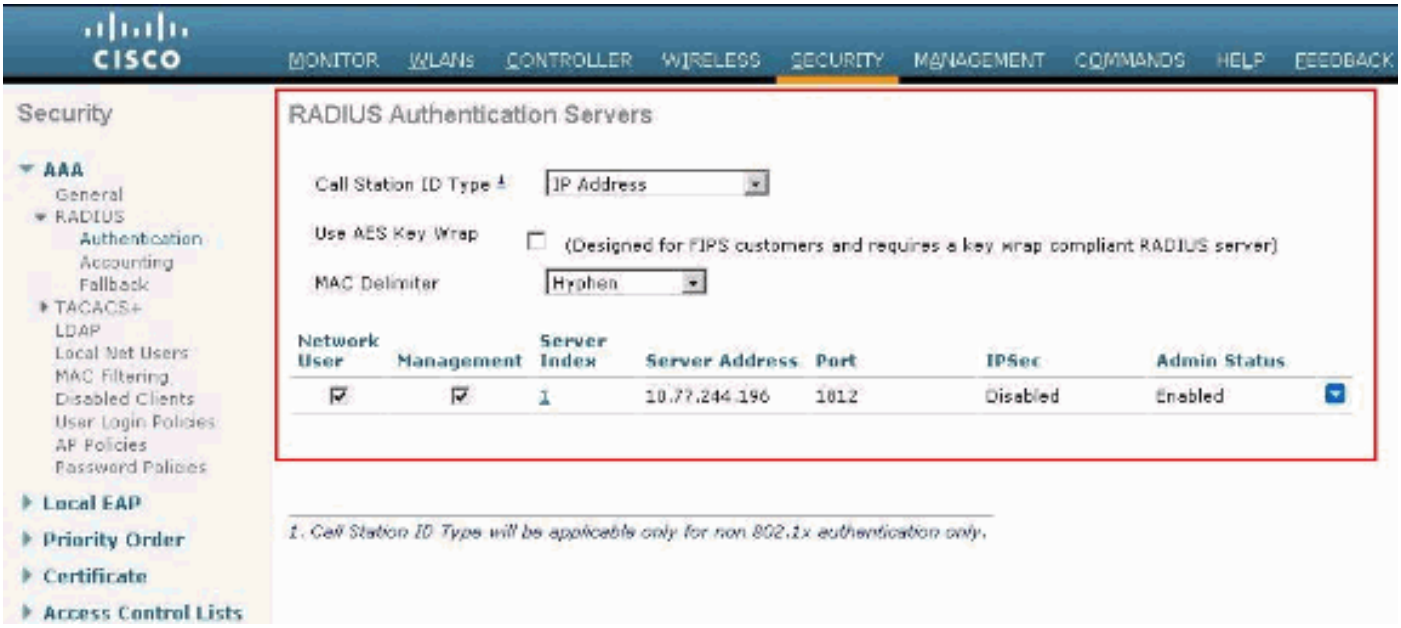
将您的 RADIUS 服务器信息输入到 Cisco WLC 中

完成这些步骤：

1. 在顶部的菜单中单击 **Security**。
2. 在左侧的菜单中单击 **Radius Authentication**。
3. 单击 **New**，并且输入 ACS/RADIUS 服务器的 IP 地址。在本例中，ACS 服务器的 IP 地址是 **10.77.244.196**。
4. 输入 RADIUS 服务器的共享密钥。确保此密钥与您在 WLC 的 RADIUS 服务器中输入的密钥相同。
5. 保留端口号为默认值 1812。
6. 确保已启用 **Server Status** 选项。
7. 选中 **Network User Enable 框**，以便使用此 RADIUS 服务器为您的无线网络中的用户验证身份。
8. 单击 **Apply**。



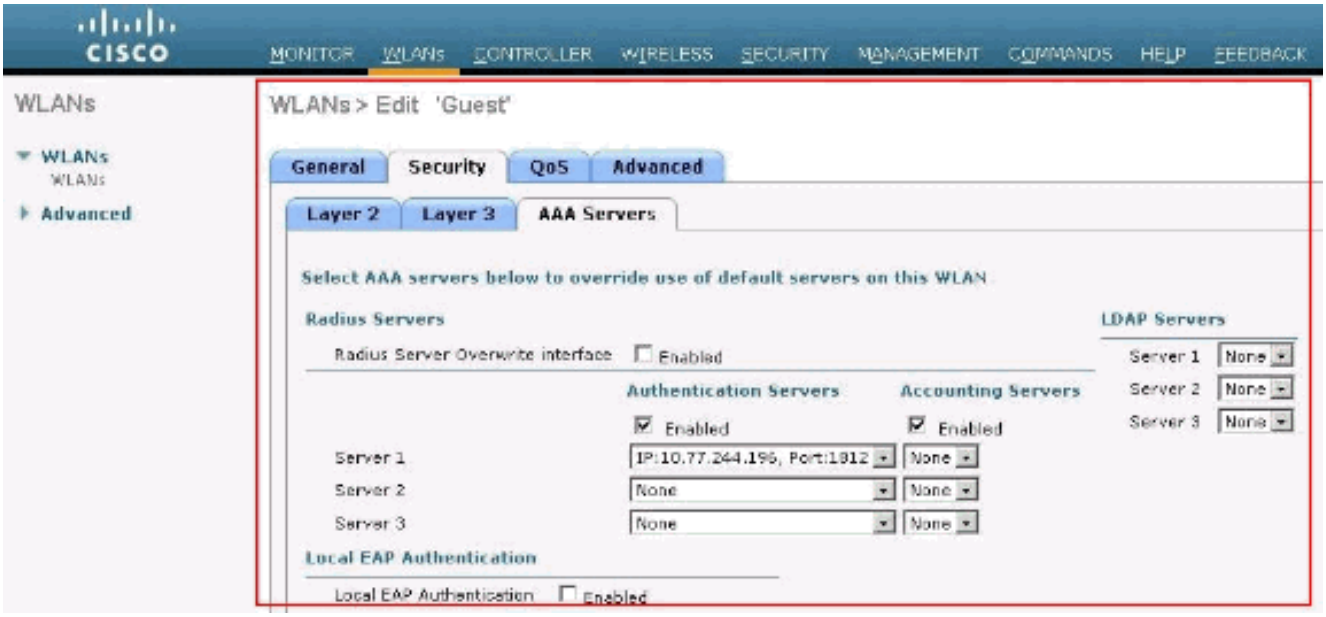
确保已选中 *Network User* 框，且已启用 *Admin Status*。



配置使用 RADIUS 服务器的 WLAN

即然已在 WLC 上配置 RADIUS 服务器，您需要配置 WLAN 以使用此 RADIUS 服务器进行 Web 身份验证。完成以下步骤以配置使用 RADIUS 服务器的 WLAN。

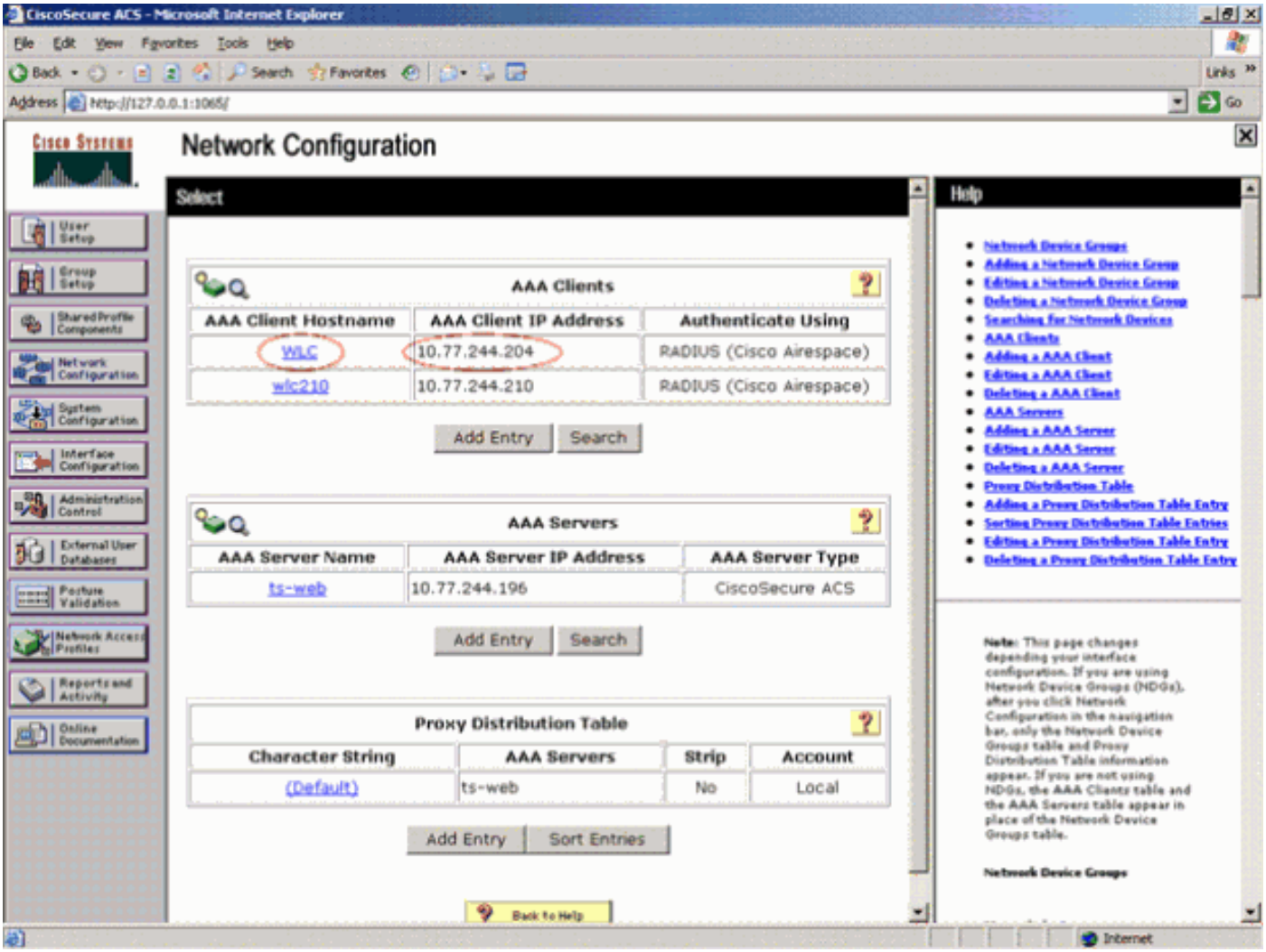
1. 打开您的 WLC 浏览器并单击 **WLANs**。这样就会显示 WLC 上配置的 WLAN 列表。点击为 Web 身份验证创建的 WLAN **访客**。
2. 在 **WLANs > Edit** 页面上，点击 **Security 菜单**。点击“Security”下的 **AAA Servers** 选项卡。然后，选择 RADIUS 服务器，在本例中为 10.77.244.196：



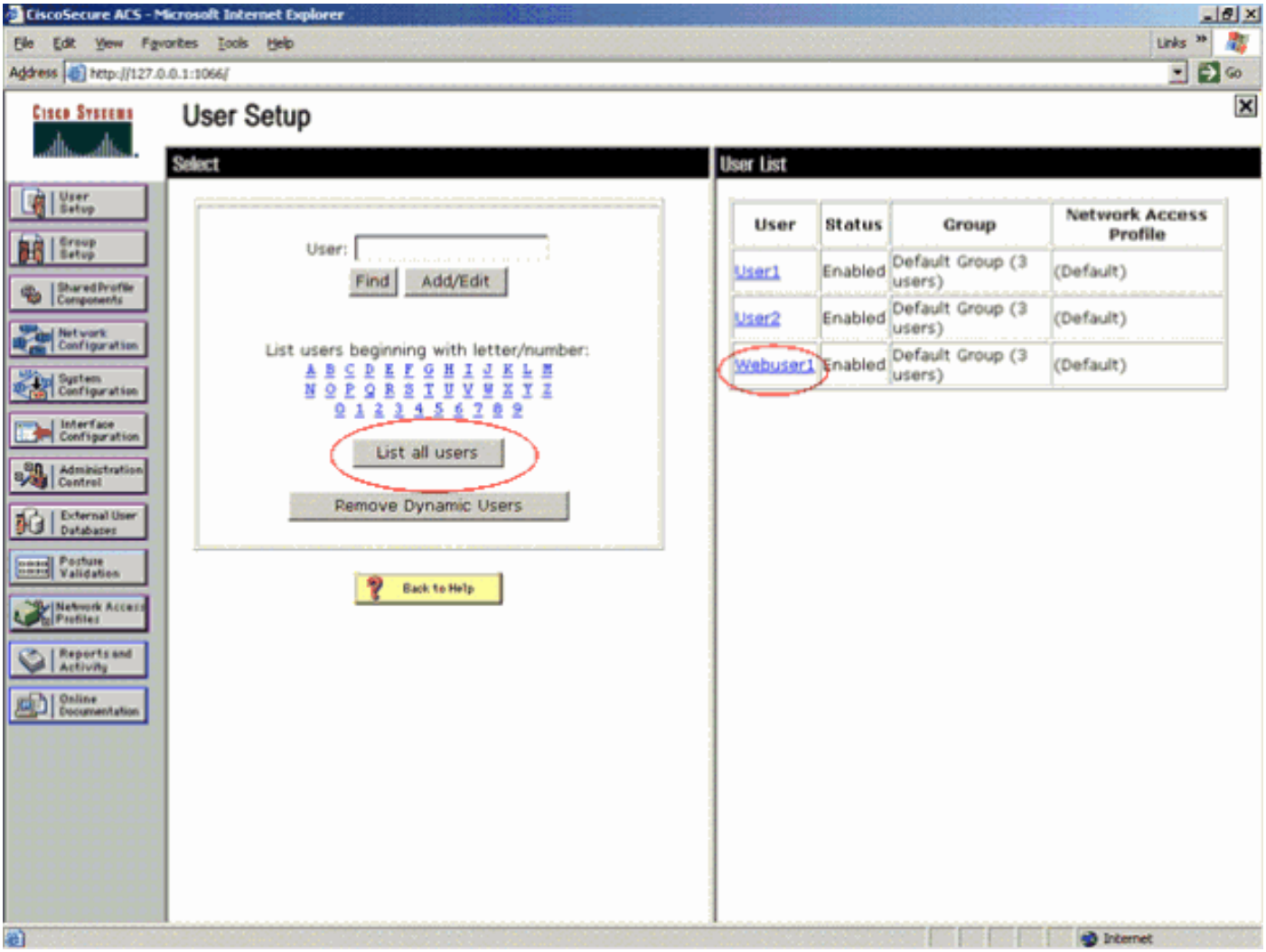
3. 单击 **Apply**。

验证 ACS

当您设置 ACS 时，请切记下载所有最新补丁程序和最新代码。这应该能够解决迫在眉睫的问题。如果您使用的是 RADIUS 身份验证，请确保您的 WLC 被列为 AAA 客户端之一。点击左侧的 **Network Configuration 菜单**以核实这一点。点击 AAA 客户端，然后验证已配置的密码和身份验证类型。有关如何配置 AAA 客户端的详细信息，请参阅“Cisco 安全访问控制服务器 4.2 用户指南”的配置 AAA 客户端部分。



当您选择用户设置时，请再次验证您的用户实际上是否存在。点击 **List All Users**。此时会显示如图所示的窗口。请确保在该列表中存在已创建的用户。

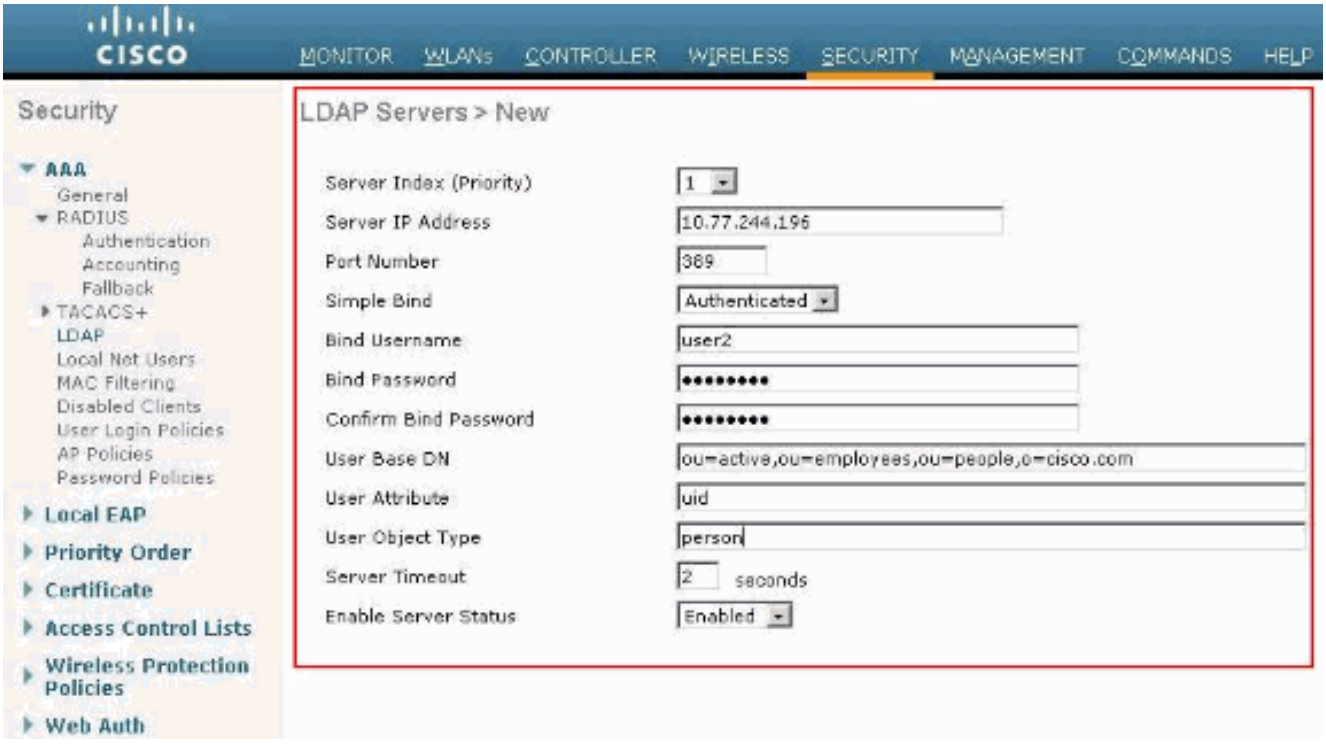


LDAP 服务器

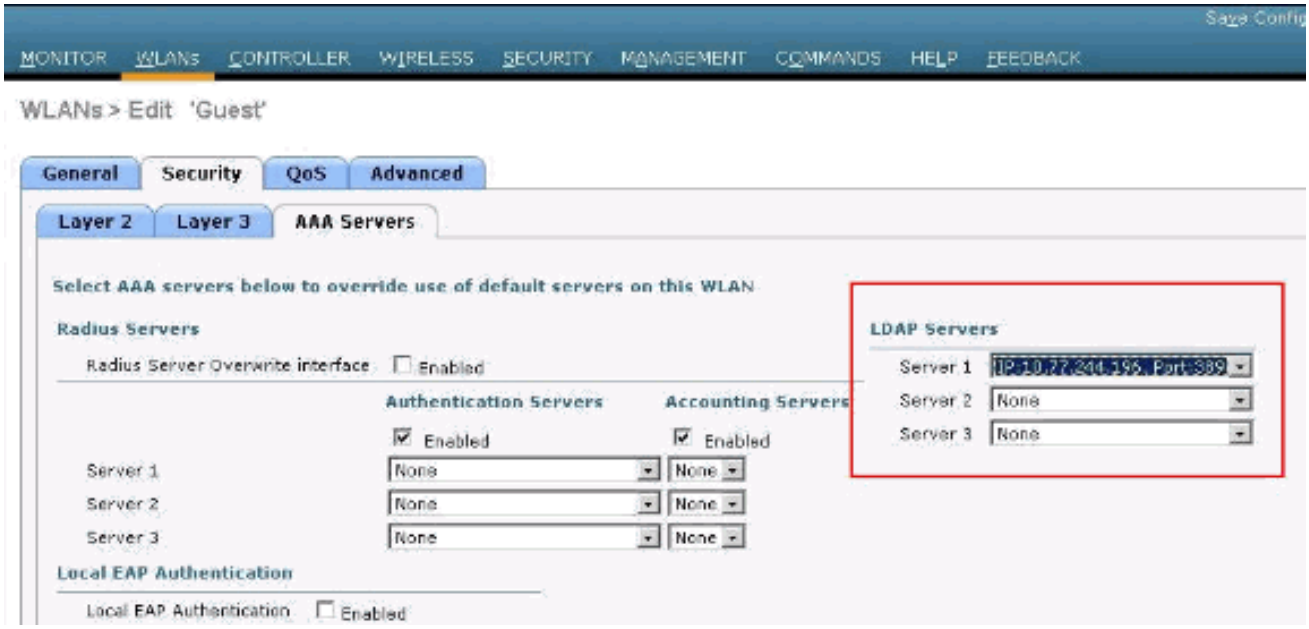
此部分介绍如何将轻量级目录访问协议 (LDAP) 服务器配置为后端数据库，类似于 RADIUS 或本地用户数据库。LDAP 后端数据库允许控制器向 LDAP 服务器查询特定用户的凭证（用户名和密码）。然后使用这些凭证对用户进行身份验证。

使用控制器 GUI 完成以下步骤以配置 LDAP：

1. 依次点击 **Security** > AAA > **LDAP** 以打开 LDAP 服务器。此页列出已配置的所有 LDAP 服务器。如果要删除现有的 LDAP 服务器，请将光标悬停到该服务器的蓝色下拉箭头上并选择 **Remove**。如果要确保控制器可访问特定服务器，请将光标悬停到该服务器的蓝色下拉箭头上并选择 **Ping**。
2. 执行下列操作之一：要编辑现有的 LDAP 服务器，请点击该服务器的索引编号。此时会显示 LDAP Servers > Edit 页面。要添加 LDAP 服务器，请点击 **New**。这会显示 **LDAP Servers > New** 页。



3. 如果要添加新服务器，请从服务器索引（优先级）下拉框中选择一个编号，以便指定此服务器相对于任何其他已配置 LDAP 服务器的优先级顺序。最多可以配置 17 个服务器。如果控制器无法访问第一个服务器，则它会尝试列表中的第二个服务器，依此类推。
4. 如果要添加新服务器，请在“Server IP Address”字段中输入 LDAP 服务器的 IP 地址。
5. 如果要添加新服务器，请在“Port Number”字段中输入 LDAP 服务器的 TCP 端口号。有效范围是 1 到 65535，默认值是 **389**。
6. 选中 **Enable Server Status** 复选框以启用此 LDAP 服务器，或者取消选中以禁用。默认值是禁用。
7. 从“Simple Bind”下拉框中选择 **Anonymous** 或 **Authenticated** 以指定 LDAP 服务器的本地身份验证绑定方法。匿名方法允许匿名访问 LDAP 服务器，而身份验证方法要求输入用户名和密码以便安全访问。默认值是 Anonymous。
8. 如果在步骤 7 选择“Authenticated”，请完成以下步骤：在“Bind Username”字段中，请输入将用于 LDAP 服务器本地身份验证的用户名。在“Bind Password”和“Confirm Bind Password”字段中，请输入将用于 LDAP 服务器本地身份验证的密码。
9. 在“User Base DN”字段中，请输入包含所有用户列表的 LDAP 服务器中的子树的可分辨名称 (DN)。例如，ou=组织单位，.ou=下一个组织单位，o=corporation.com。如果包含用户的树是基本 DN，请键入 o=corporation.com 或 dc=corporation，dc=com。
10. 在 **User Attribute** 字段中，输入包含用户名的用户记录中的属性名称。您可从目录服务器获取此属性。
11. 在 **User Object Type** 字段中，输入将记录标识为用户的 LDAP objectType 属性的值。通常，用户记录具有多个 objectType 属性值，其中有些对用户是唯一的，而另一些则与其他对象类型共享。
12. 在“Server Timeout”字段中，请输入重发之间的秒数。有效范围是 2 到 30 秒，默认值是 2 秒。
13. 单击 **Apply** 以提交更改。
14. 点击 **Save Configuration** 保存您的更改。
15. 如果希望将特定 LDAP 服务器分配到 WLAN，请完成以下步骤：单击“WLANs”以打开“WLANs”页。点击所需 WLAN 的 ID 编号。当显示 WLANs > Edit 页面时，依次点击 **Security** >AAA **Servers** 选项卡以打开 WLAN > Edit (Security > AAA Servers) 页面。



从 LDAP 服务器下拉框中选择要与此 WLAN 一起使用的 LDAP 服务器。您可以选择最多三个 LDAP 服务器，按优先级顺序尝试。单击 **Apply** 以提交更改。点击 **Save Configuration** 保存您的更改。

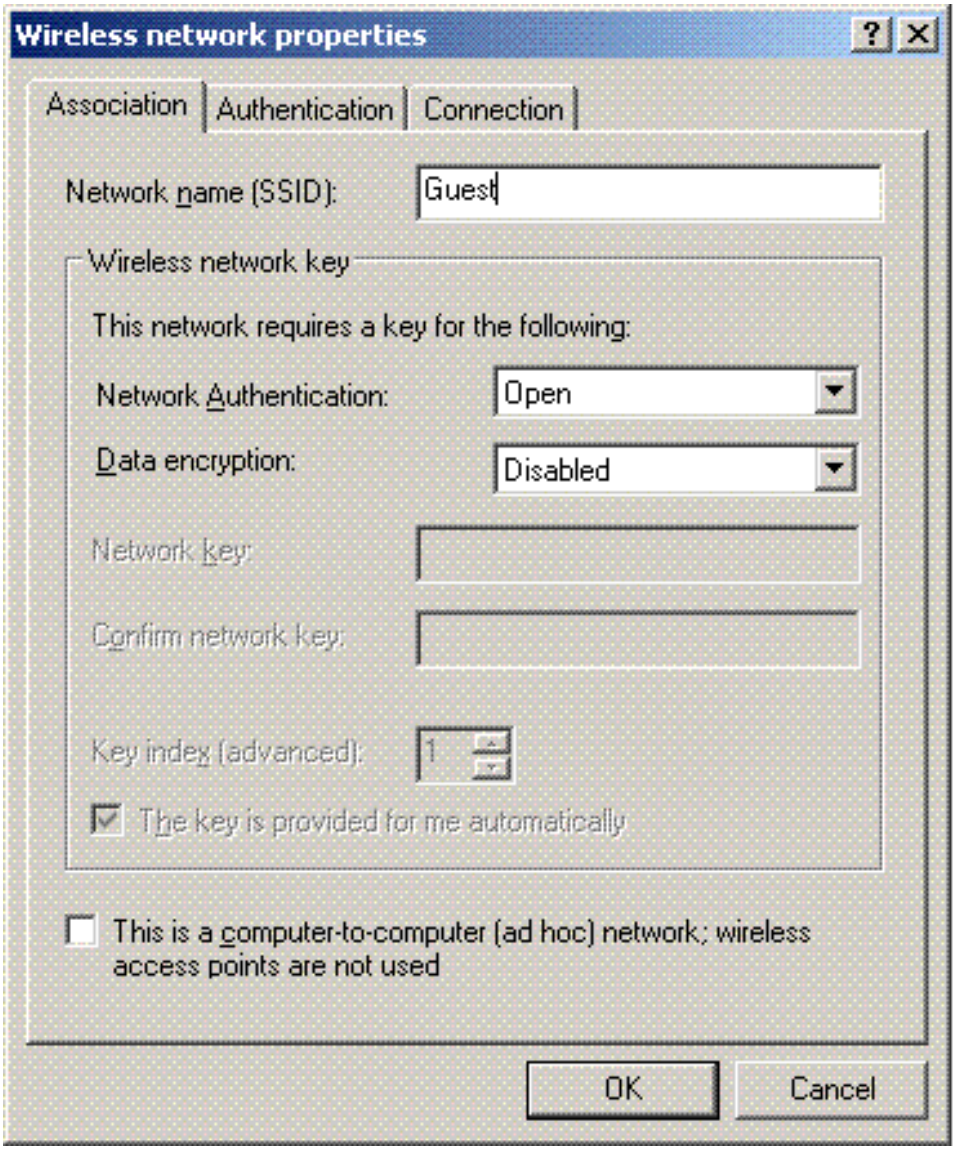
配置您的 WLAN 客户端以使用 Web 身份验证

配置 WLC 之后，客户端必须适当配置以进行 Web 身份验证。本部分提供有关如何配置用于 Web 身份验证的 Windows 系统的信息。

客户端配置

对此用户而言，Microsoft 无线客户端配置保持大致不变。您只需要添加适当的 WLAN/SSID 配置信息。完成这些步骤：

1. 从 Windows“开始”菜单中选择**设置 > 控制面板 > 网络和 Internet 连接**。
2. 单击**网络连接**图标。
3. 右键单击 **LAN 连接**图标并选择“禁用”。
4. 右键单击**无线连接**图标并选择“启用”。
5. 再次右键单击**无线连接**图标并选择“属性”。
6. 从“无线网络连接属性”窗口中，单击**无线连接**选项卡。
7. 在首选网络区域下单击**添加**以配置 Web 身份验证 SSID。
8. 在“关联”选项卡下，输入要用于 Web 身份验证的网络名称 (WLAN/SSID) 值。



Note: 默认情况下，数据加密为有线等效加密 (WEP)。请禁用数据加密以使 Web 身份验证能够正常运行。

9. 在窗口底部单击**确定**以保存配置。当您与 WLAN 通信时，您会在“首选网络”框中看到一个信号图标。

这表示 Web 身份验证无线连接成功。WLC 已为您的无线 Windows 客户端提供 IP 地址。

Note: 如果您的无线客户端也是 VPN 终端，并将 Web 身份验证配置为 WLAN 的一个安全功能，则在您完成此处所述的 Web 身份验证过程之前不会建立 VPN 隧道。为了建立 VPN 隧道，客户端必须先成功完成 Web 身份验证过程。只有在那时才能成功建立 VPN 隧道。

Note: 在成功登录之后，如果无线客户端空闲，并且不与任何其他设备通信，则在超过空闲超时期限之后客户端会取消身份验证。默认情况下，超时期限为 300 秒，可以使用以下 CLI 命令进行更改：config network usertimeout<seconds>。当发生这种情况时，客户端条目会从控制器中删除。如果客户端再次关联，它将切换回 Webauth_Reqd 状态。

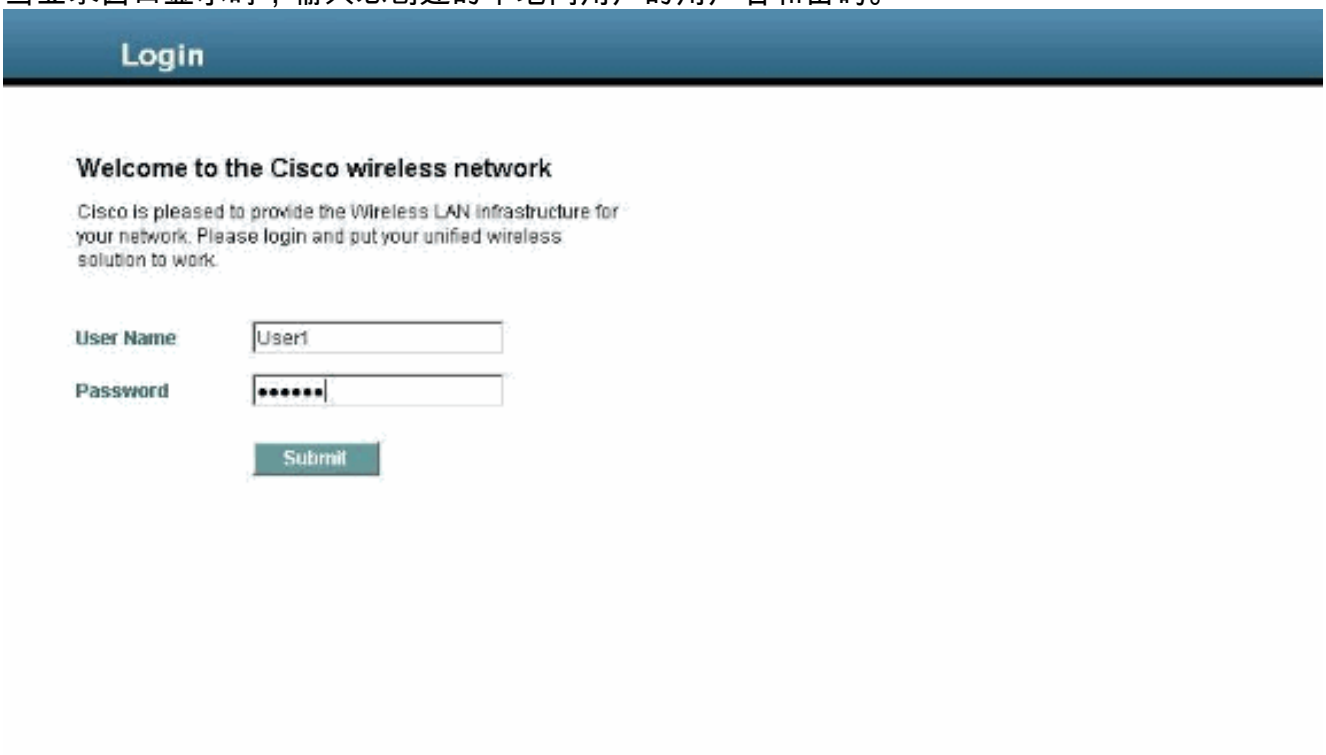
Note: 如果客户端在成功登录后保持活动状态，则在该 WLAN 上配置的会话超时期限之后，它们将取消验证，且条目仍会从控制器中删除（例如，默认为 1800 秒，并可使用以下 CLI 命令来更改：config wlan session-timeout <WLAN ID> <seconds>）。当发生这种情况时，客户端条目会从控制器中删除。如果客户端再次关联，它将切换回 Webauth_Reqd 状态。

如果客户端处于 Webauth_Reqd 状态，则不管它们是活动还是空闲，客户端在 **Web 身份验证要求的超时期限**（例如，300 秒，用户不可以配置此时间）之后会取消验证。来自客户端的所有流量（通过 Pre-Auth ACL 允许）都将中断。如果客户端再次关联，它将切换回 Webauth_Reqd 状态。

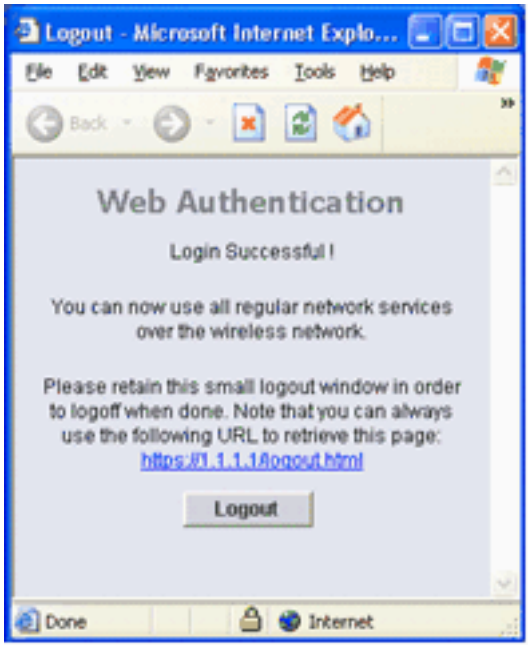
客户端登录

完成这些步骤：

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。如果控制器运行早于 3.0 的任何版本，则用户必须输入 https://1.1.1.1/login.html 才能显示 Web 身份验证页面。此时将显示安全警报窗口。
2. 单击 **Yes** 以继续操作。
3. 当登录窗口显示时，输入您创建的本地网用户的用户名和密码。



如果登录成功，您将看到两个浏览器窗口。如果显示更大的窗口，则表示成功登录，您可以使用此窗口浏览互联网。完成对访客网络的使用时，可使用较小的窗口注销。该屏幕截图显示了 Web 身份验证的成功重定向。下一张屏幕截图显示“登录成功”窗口，该窗口显示何时进行身份

验证。 

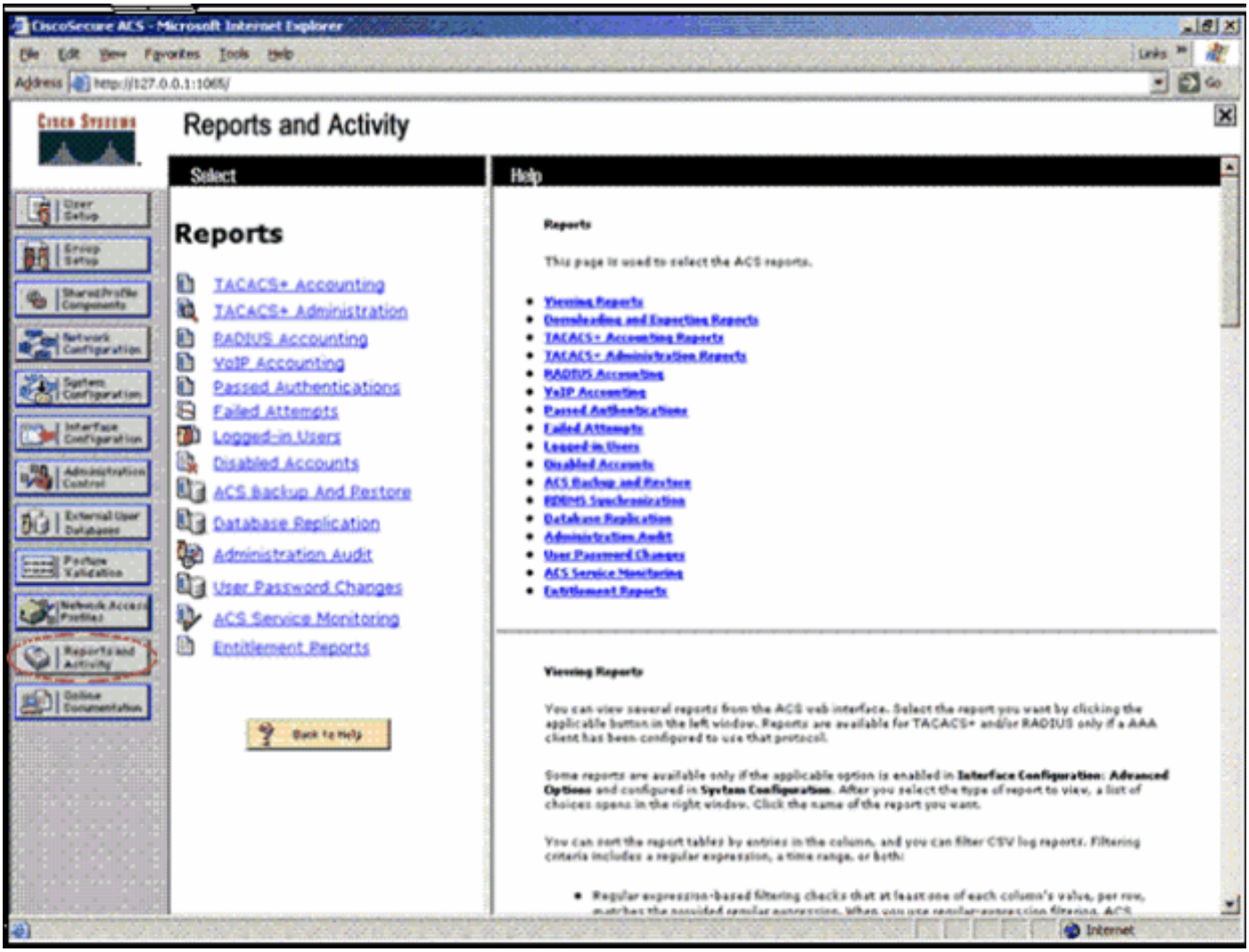
思科 4404/WiSM 控制器可以支持 125 个 Web 身份验证用户同时登录，并且可扩展到 5000 个 Web 身份验证客户端。

思科 5500 控制器可以支持 150 个 Web 身份验证用户同时登录。

Web 身份验证故障排除

ACS 故障排除

如果口令验证存在问题，请单击 ACS 左下方的 **Reports and Activity** 以打开所有可用的报告。打开报告窗口后，可以通过相应选项打开 RADIUS 记账、失败的尝试登录、通过的验证、已登录用户和其他报告。这些报告为 .csv 文件，您可以在计算机上本地打开这些文件。这些报告有助于揭示身份验证存在的问题，如用户名和/或口令不正确。ACS 还附带联机文档。如果未连接到真实网络并且未定义服务端口，ACS 将使用以太网端口的 IP 地址作为服务端口。如果您的网络未建立连接，您很可能最终使用 Windows 默认 IP 地址 169.254.x.x。



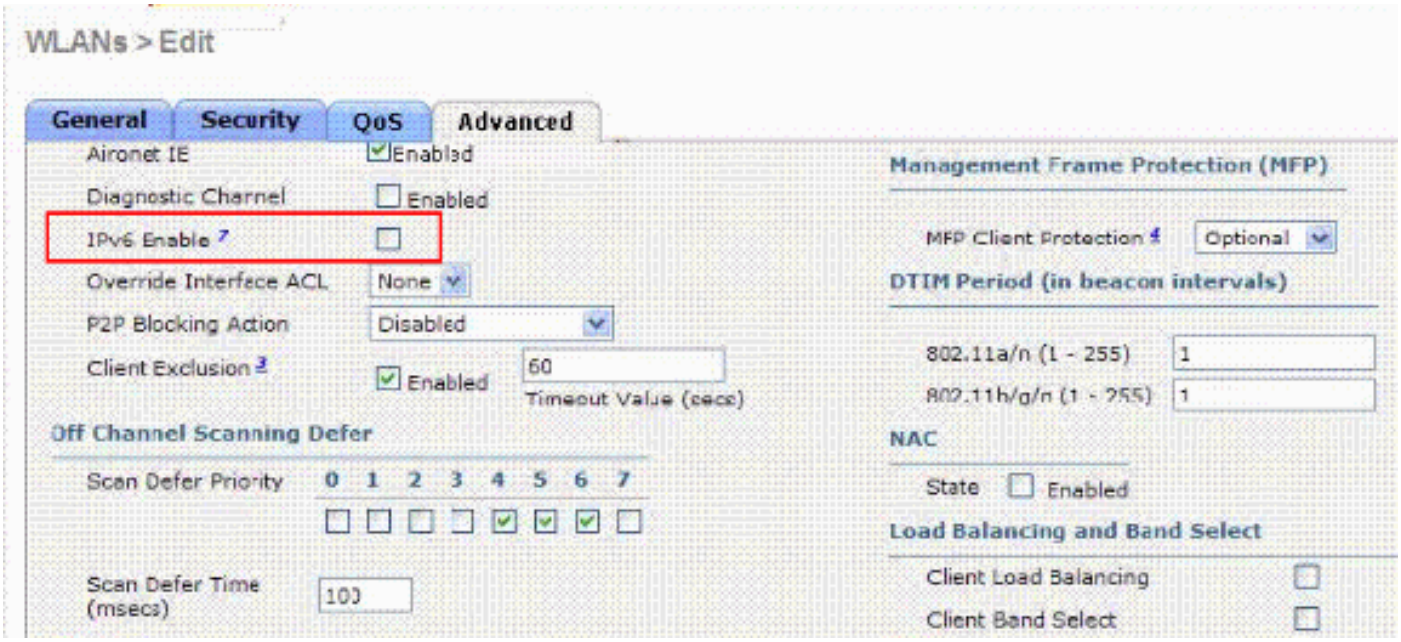
Note: 如果键入任何外部 URL，WLC 会自动将您连接到内部 Web 身份验证页。如果自动连接不起作用，您可以在 URL 栏中输入 WLC 的管理 IP 地址以排除故障。在浏览器顶部查找说明 Web 身份验证重定向的消息。

请参阅无线 LAN 控制器 (WLC) 上的 Web 身份验证故障排除，了解有关 Web 身份验证故障排除的详细信息。

与 IPv6 桥接的 Web 身份验证

为了配置 WLAN 以用于 IPv6 桥接，请从控制器 GUI 导航至 **WLAN**。然后，选择所需的 WLAN 并从 **WLANs** > Edit 页面选择 **Advanced**。

如果要使连接到此 WLAN 的客户端可接受 IPv6 数据包，请选择 **IPv6 Enable 复选框**。否则，请不要选中该复选框，这是默认值。如果禁用（或取消选中）IPv6 复选框，则将仅在身份验证之后才允许使用 IPv6。启用 IPv6 则意味着控制器可传递 IPv6 流量，无需进行客户端身份验证。



有关 IPv6 桥接的更详细信息和**使用此功能的准则**，请参阅《思科无线 LAN 控制器配置指南》第 7 版中的配置 IPv6 桥接部分。

Related Information

- 使用无线局域网控制器的外部 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
- Cisco 无线 LAN
- 使用 Cisco WLAN 控制器的有线访客接入配置示例
- 思科无线 LAN 控制器配置指南，第 7.0 版 - 管理用户帐户
- 通过 RADIUS 服务器对无线局域网控制器的公用入口管理员执行身份验证
- Technical Support & Documentation - Cisco Systems