使用WLC配置外部Web身份验证

目录

简介

本文档介绍如何使用外部 Web 服务器设置无线 LAN 控制器 (WLC) 以进行 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
- 轻量接入点协议(LWAPP)及无线接入点的控制和调配(CAPWAP)基础知识
- 有关如何设置和配置外部 Web 服务器的知识
- 有关如何设置和配置 DHCP 和 DNS 服务器的知识

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 7.0.116.0 的 Cisco 4400 WLC
- 思科1131AG系列LAP
- 运行固件版本3.6的思科802.11a/b/g无线客户端适配器
- 托管 Web 身份验证登录页面的外部 Web 服务器
- 用于地址解析和为无线客户端分配 IP 地址的 DNS 和 DHCP 服务器

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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

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。Web身份验证是一种简单的身份验证方法，不需要请求方或客户端实用程序。

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

本文提供配置示例以说明如何配置 WLC 使用外部 Web 服务器上的登录脚本。

外部 Web 身份验证过程

使用外部Web身份验证时，用于Web身份验证的登录页存储在外部Web服务器上。下面是无线客户端尝试接入启用了外部 Web 身份验证的 WLAN 网络时的事件顺序：

1. 客户端（最终用户）连接到WLAN并打开Web浏览器并输入URL，例如www.cisco.com。
2. 客户端向DNS服务器发送DNS请求以将www.cisco.com解析为IP地址。
3. WLC将请求转发到DNS服务器，DNS服务器反过来会将www.cisco.com解析为IP地址并发送DNS应答。控制器将应答转发给客户端。
4. 客户端尝试通过www.cisco.com IP地址发起TCP连接，方法是将TCP SYN数据包发送到www.cisco.com IP地址。
5. 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。
6. 客户端向 www.google.com 发送 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。
7. 然后，客户端启动与重定向URL的HTTPS连接，重定向URL将其发送到1.1.1.1。这是控制器的虚拟IP地址。客户端必须验证或忽略服务器证书，以建立 SSL 隧道。
8. 由于已启用外部Web身份验证，因此WLC会将客户端重定向到外部Web服务器。

9. 外部Web身份验证登录URL附加了参数，例如AP_Mac_Address、client_url(www.cisco.com)和客户端联系控制器Web服务器所需的action_URL。**注意**：action_URL告知Web服务器用户名和密码存储在控制器上。凭证必须发送回控制器才能进行身份验证。
10. 外部 Web 服务器 URL 可将用户定向到登录页。
11. 登录页面接受用户凭证输入，并将请求发送回WLC Web服务器的action_URL，例如http://1.1.1.1/login.html。
12. WLC Web 服务器提交用于身份验证的用户名和口令。
13. WLC 启动 RADIUS 服务器请求或使用 WLC 上的本地数据库并对用户进行身份验证。
14. 如果身份验证成功，WLC Web 服务器会将用户转送至已配置的重定向 URL 或客户端最初使用的 URL（例如 www.cisco.com）。
15. 如果身份验证失败，则 WLC Web 服务器会将用户重定向回客户登录 URL。

注意：要将外部Web身份验证配置为使用HTTP和HTTPS以外的端口，请发出以下命令：

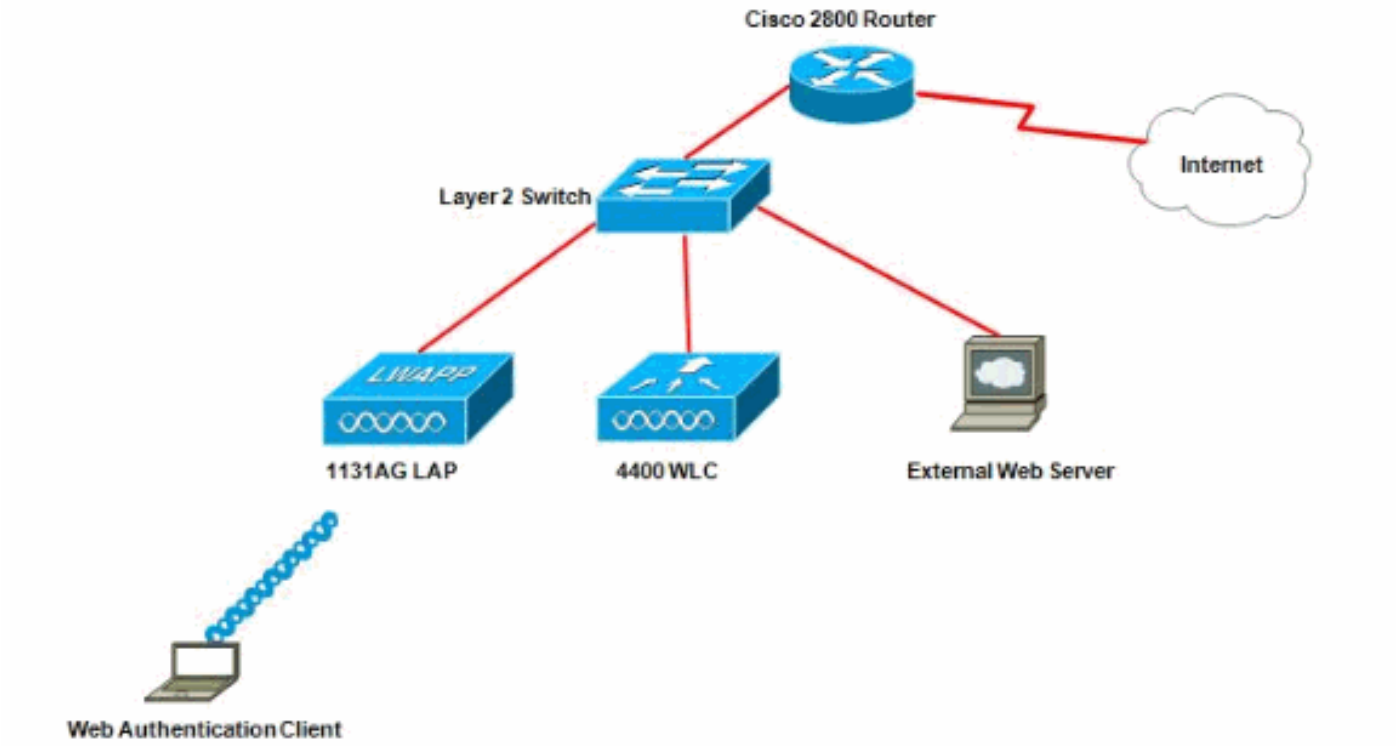
```
(Cisco Controller) >config network web-auth-port

<port>          Configures an additional port to be redirected for web authentication.
```

网络设置

配置示例使用此设置。WLC 上已注册 LAP。您需要为来宾用户配置一个 WLAN 来宾并必须为用户启用 Web 身份验证。您还需要确保控制器将用户重定向到外部Web服务器URL（用于外部Web身份验证）。外部 Web 服务器托管用于身份验证的 Web 登录页。

必须对照控制器上维护的本地数据库来验证用户凭证。在成功进行身份验证后，应该允许用户访问 WLAN 来宾。需要为此设置配置控制器和其他设备。

注意：您可以使用将用于Web身份验证的自定义版本的登录脚本。您可以从Cisco Software Downloads页面下载示例Web身份验证脚本。例如，对于4400控制器，导航到**产品>无线>无线LAN控制器>独立控制器> Cisco 4400系列无线LAN控制器> Cisco 4404无线LAN控制器>机箱上的软件>无线LAN控制器Web身份验证捆绑包–1.0.1**并下载**webauth_bundle.zip**文件。



注意：自定义Web身份验证捆绑包的文件名限制最多为30个字符。确保捆绑包内的文件名不超过30个字符。

注意：本文档假设已配置DHCP、DNS和外部Web服务器。有关如何配置 DHCP、DNS 和外部 Web 服务器的信息，请参阅相应的第三方文档。

配置

在您为外部 Web 身份验证配置 WLC 之前，您必须针对基本操作来配置 WLC 并将 LAP 注册到该 WLC。本文档假设已配置 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以实现LAP基本操作的新用户，请参阅轻量AP(LAP)注册到无线LAN控制器(WLC)。

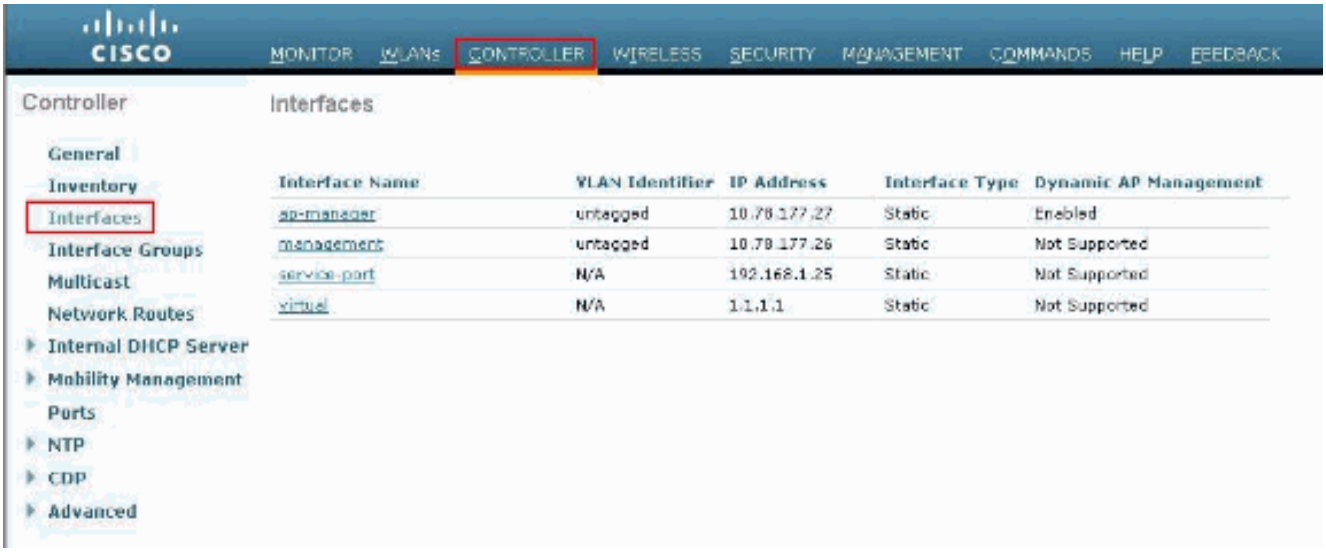
若要针对此设置配置 LAP 和 WLC，请完成以下步骤：

1. 为来宾用户创建动态接口
2. 创建预身份验证ACL
3. 在 WLC 上为来宾用户创建本地数据库
4. 配置外部 Web 身份验证的 WLC
5. 为来宾用户配置 WLAN

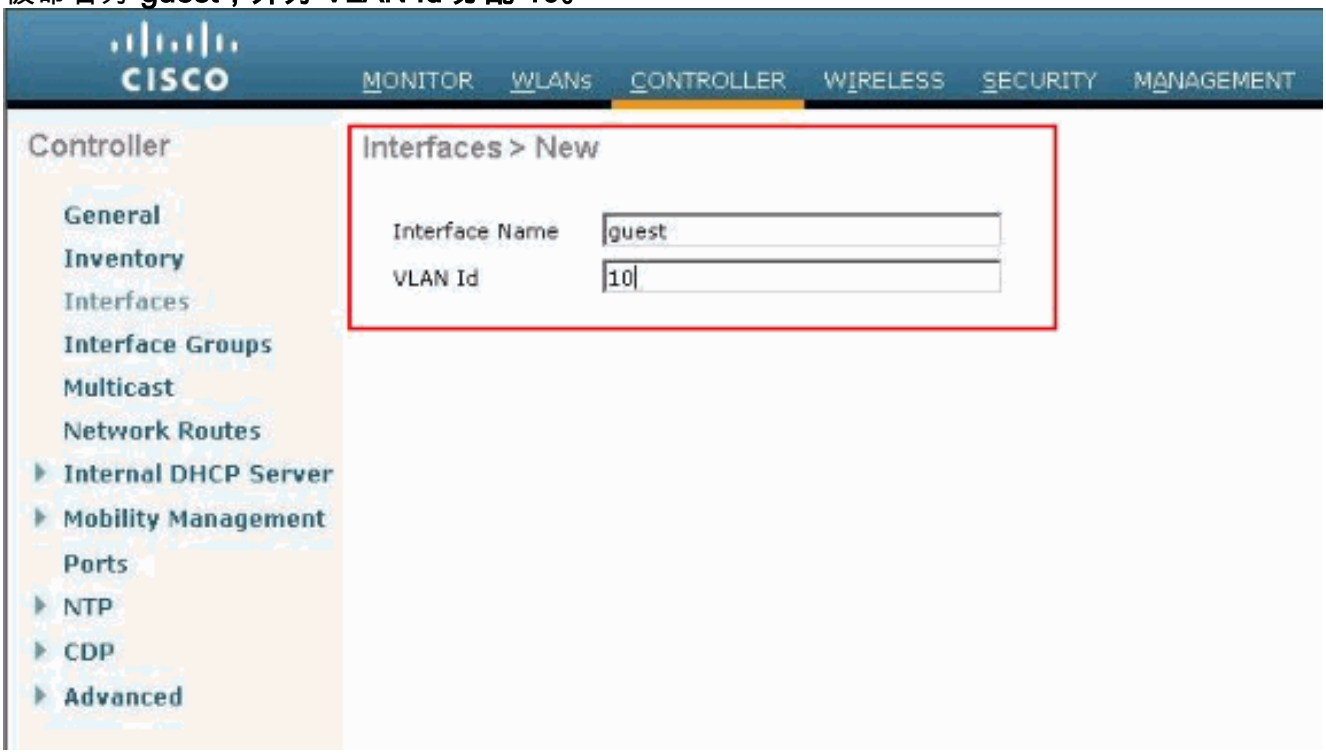
为来宾用户创建动态接口

要为来宾用户创建动态接口，请完成以下步骤：

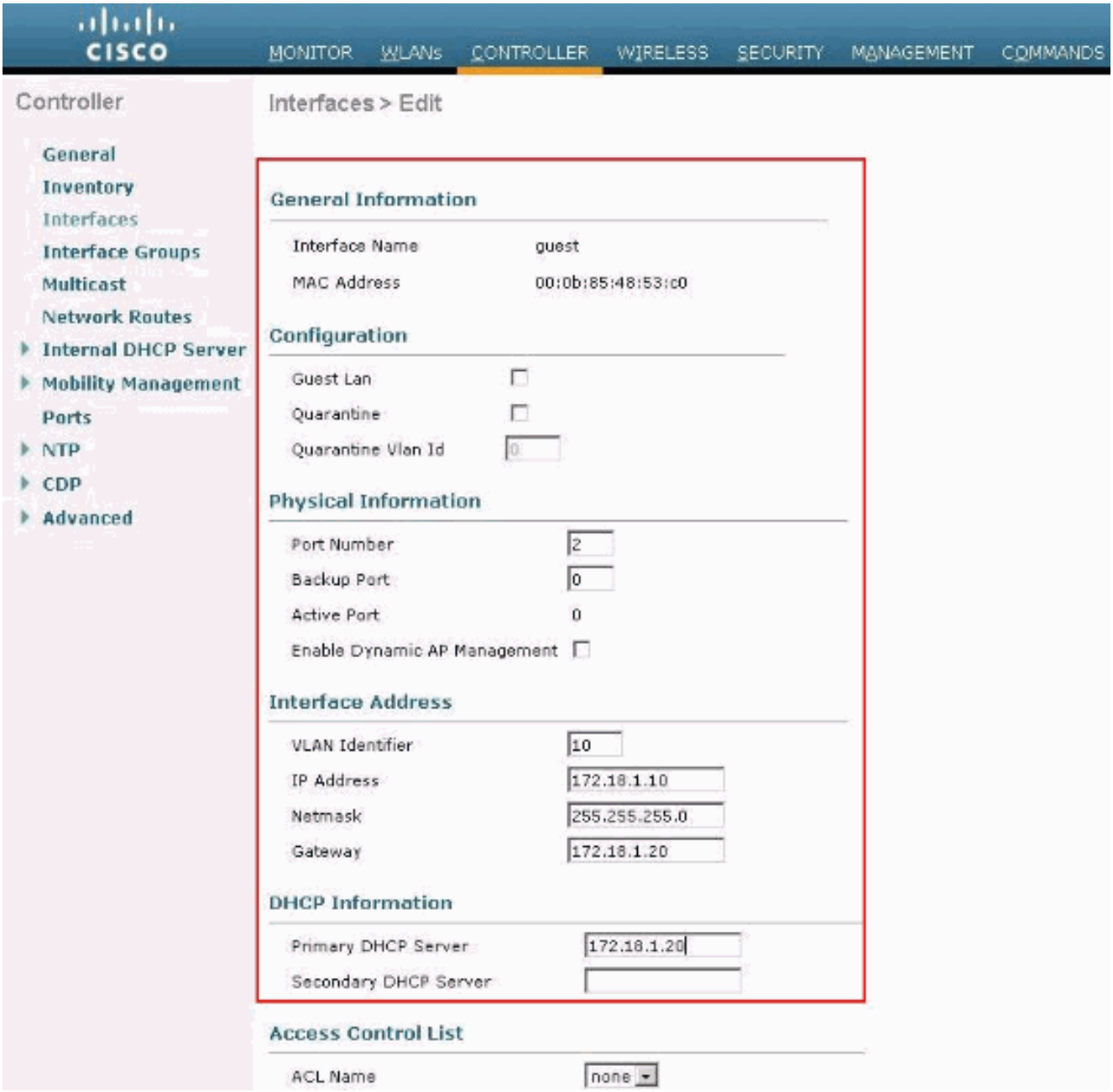
1. 从 WLC GUI 中，选择 **Controllers > Interfaces**。此时会显示“Interfaces”窗口。此窗口中会列出在控制器上配置的接口。这包括默认接口，包括管理接口、ap-manager 接口、虚拟接口和服务端口接口以及用户定义的动态接口。



2. 单击 **New 创建新的动态接口。**
3. 在**Interfaces > New**窗口中，输入接口名称和VLAN ID。然后单击**Apply**。在本例中，动态接口被命名为 **guest，并为 VLAN Id 分配 10。**



4. 对于动态接口，在 Interfaces > Edit 窗口中输入 IP 地址、子网掩码和默认网关。将它分配到 WLC 上的某个物理端口，再输入 DHCP 服务器的 IP 地址。然后，单击 **Apply**。



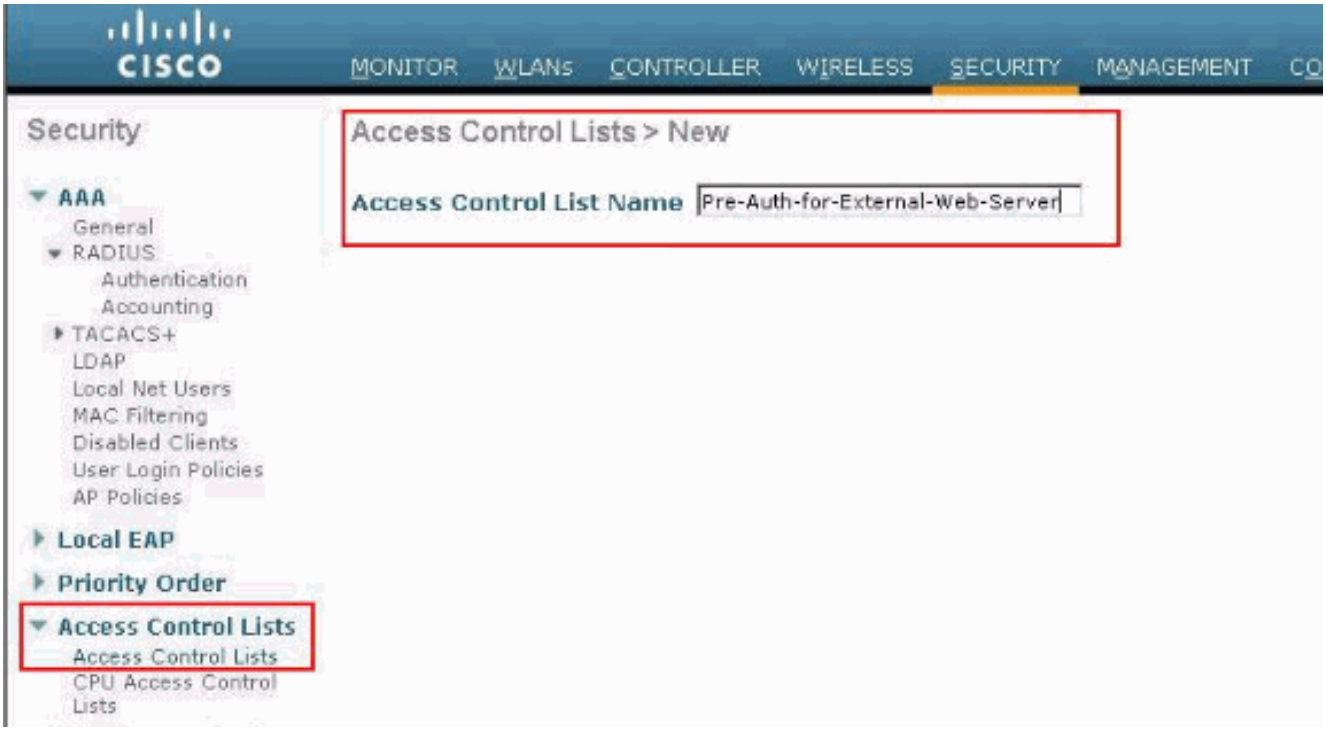
创建预身份验证ACL

使用外部Web服务器进行Web身份验证时，某些WLC平台需要为外部Web服务器（Cisco 5500系列控制器、Cisco 2100系列控制器、Cisco 2000系列和控制器网络模块）提供预身份验证ACL。对于其他WLC平台，预身份验证ACL不是必需的。

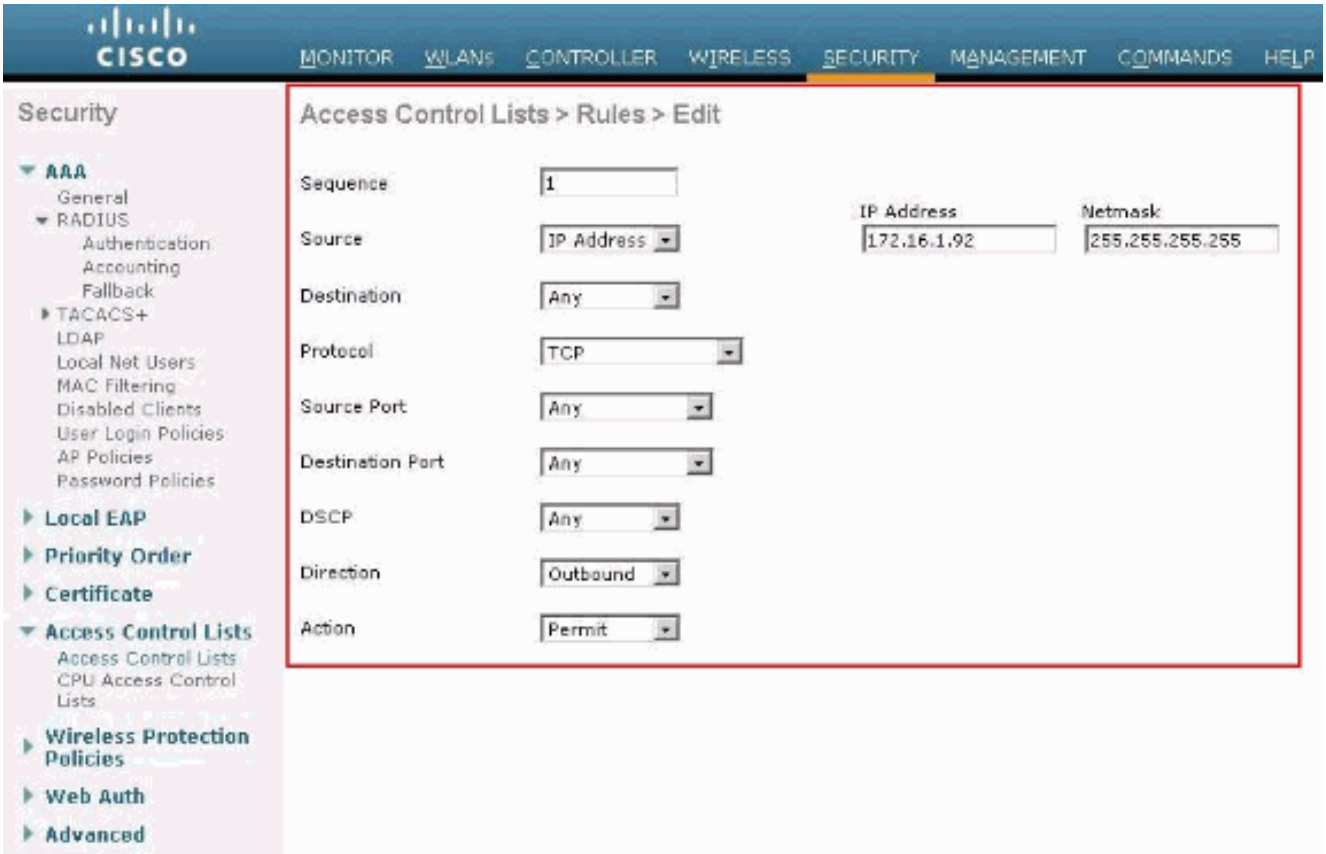
但是，在使用外部Web身份验证时，最好为外部Web服务器配置预身份验证ACL。

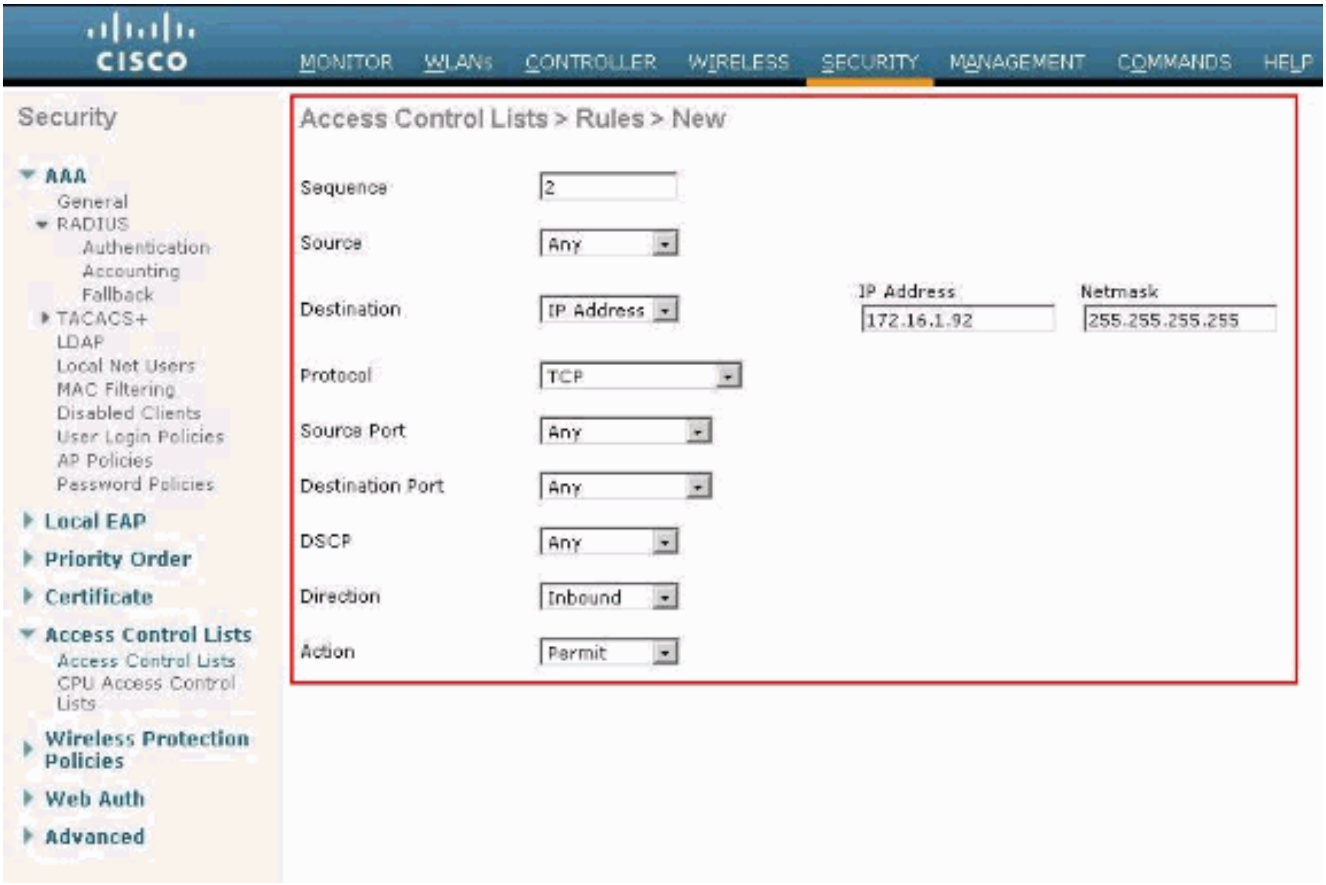
完成以下这些步骤，以便为 WLAN 配置预身份验证 ACL：

1. 从 WLC GUI 中，选择 **Security > Access Control Lists**。此窗口允许您查看类似于标准防火墙 ACL 的当前 ACL。
2. 单击 **New 以创建新的 ACL。**
3. 输入 ACL 的名称并单击 **Apply**。在本示例中，ACL命名为**Pre-Auth-for-External-Web-Server**。

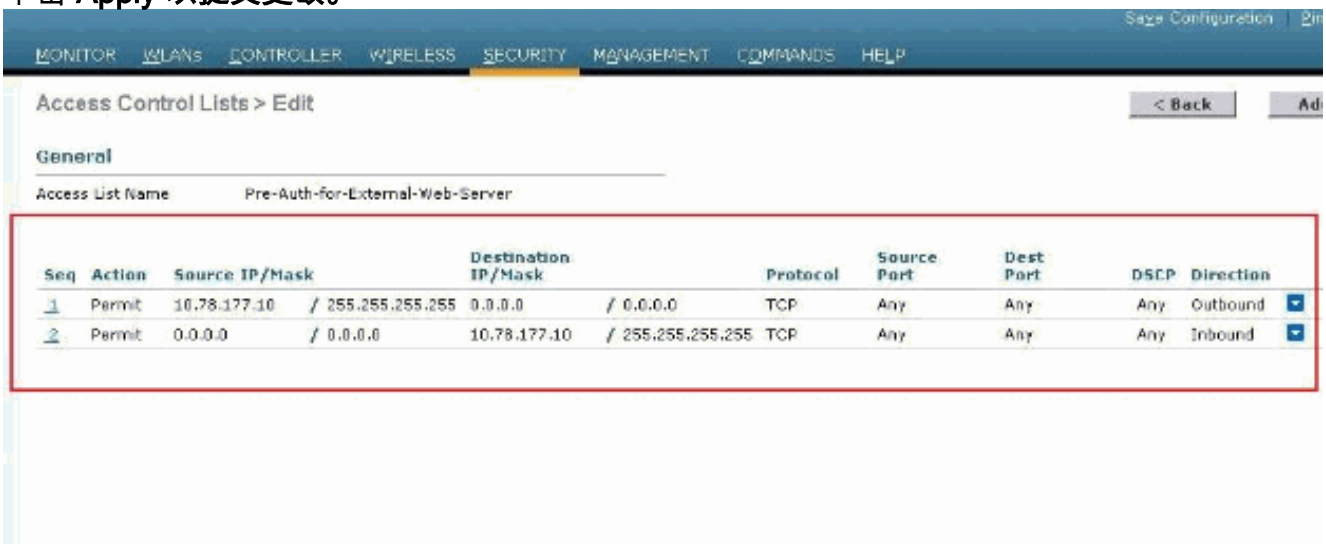


4. 对于创建的新 ACL，单击 **Edit**。此时将显示 ACL > Edit 窗口。此窗口允许用户定义新规则或修改现有 ACL 的规则。
5. 单击 **Add New Rule**。
6. 定义允许客户端访问外部 Web 服务器的 ACL 规则。在本例中，172.16.1.92 是外部 Web 服务器 IP 地址。





7. 单击 **Apply** 以提交更改。



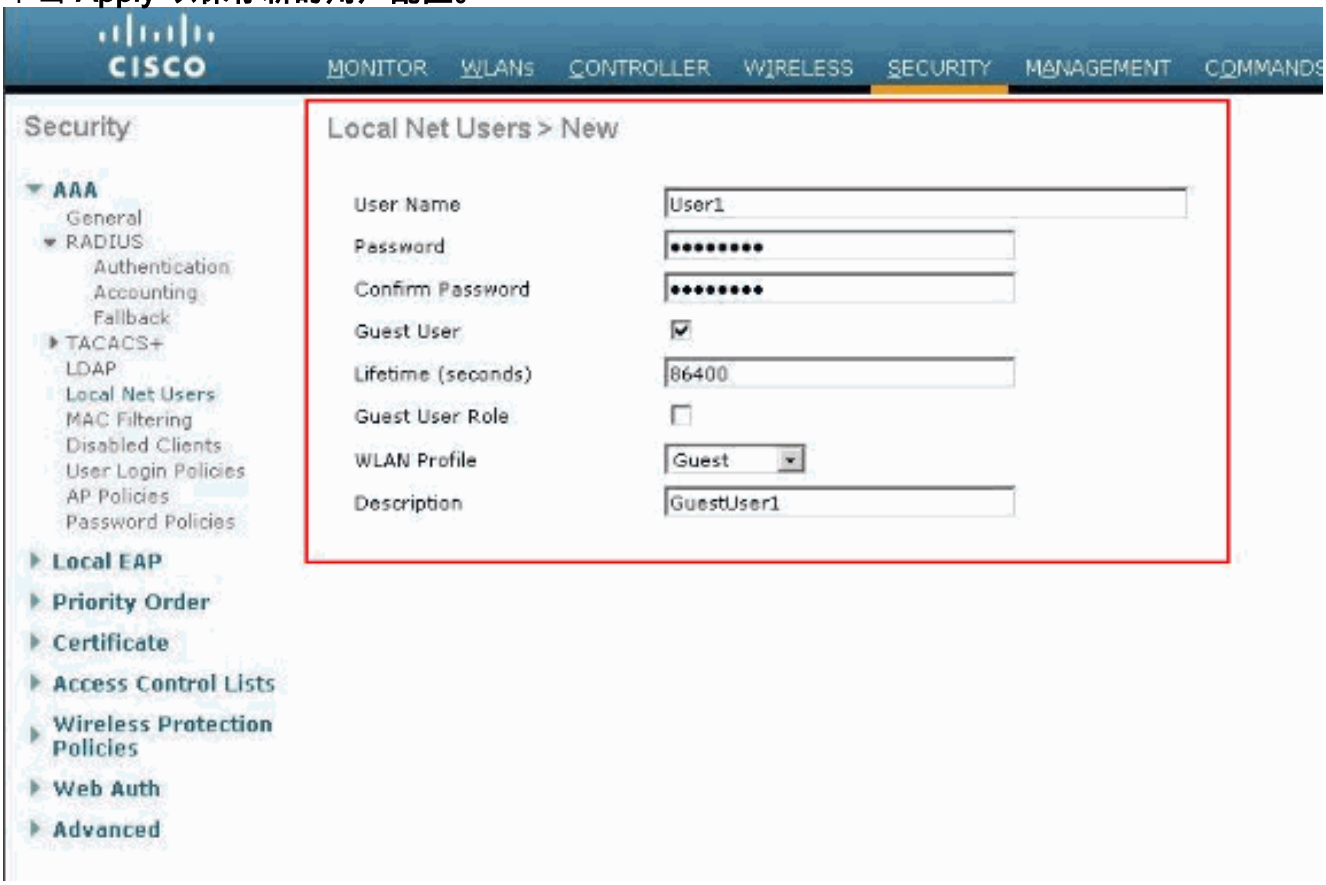
在 WLC 上为来宾用户创建本地数据库

访客用户的用户数据库可以存储在无线局域网控制器的本地数据库中，也可以存储在控制器的外部。

在本文档中，控制器上的本地数据库用于对用户进行身份验证。您必须创建本地网络用户并定义Web身份验证客户端登录的密码。要在 WLC 上创建用户数据库，请完成以下步骤：

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。**

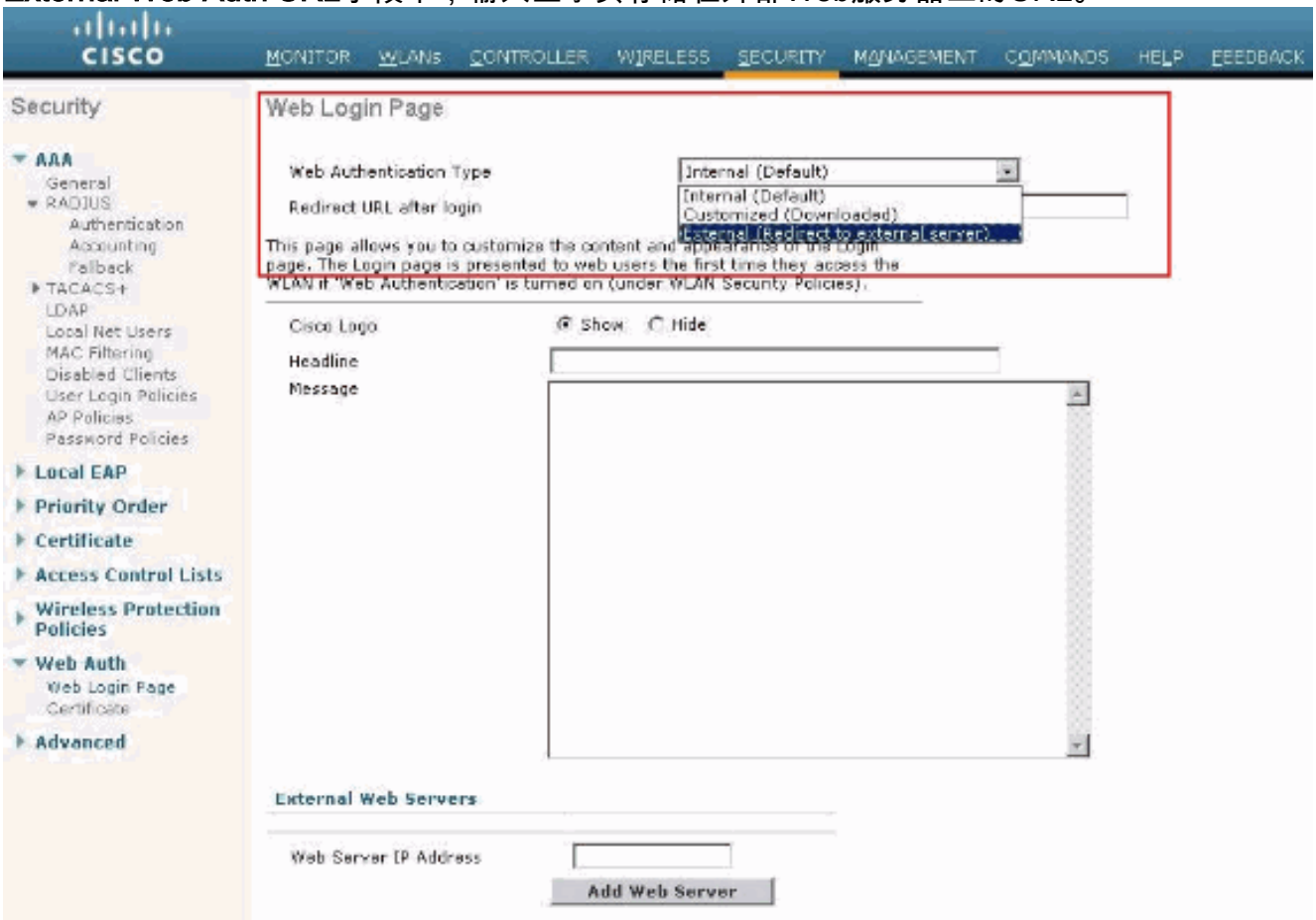


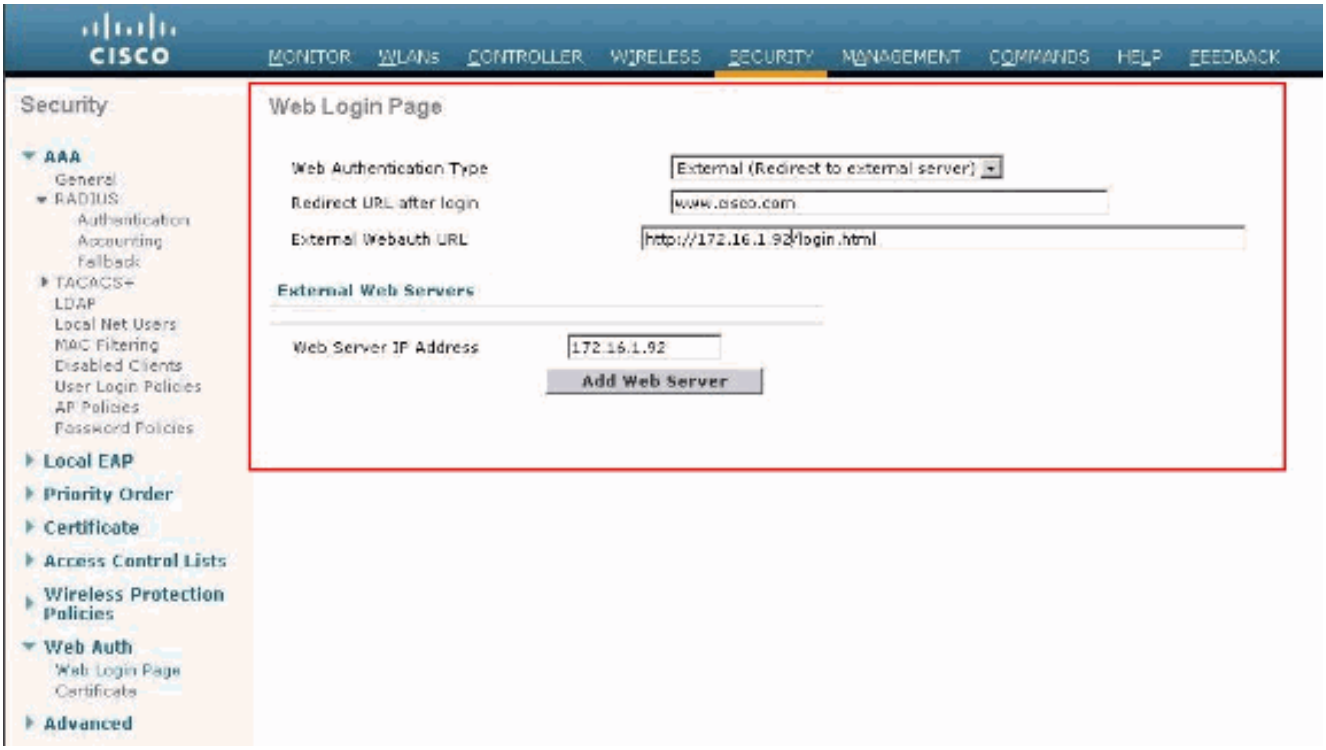
7. 重复步骤 3-6 以向数据库中添加更多用户。

配置外部 Web 身份验证的 WLC

下一步是为外部Web身份验证配置WLC。请完成以下步骤：

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. 从 Web Authentication Type 下拉框中，选择 **External (Redirect to external server)**。
3. 在**外部Web服务器**部分中，添加新的外部Web服务器。
4. 在**登录后重定向URL**字段中，输入最终用户在身份验证成功后将重定向到的页面的URL。在**External Web Auth URL**字段中，输入登录页存储在外部Web服务器上的URL。



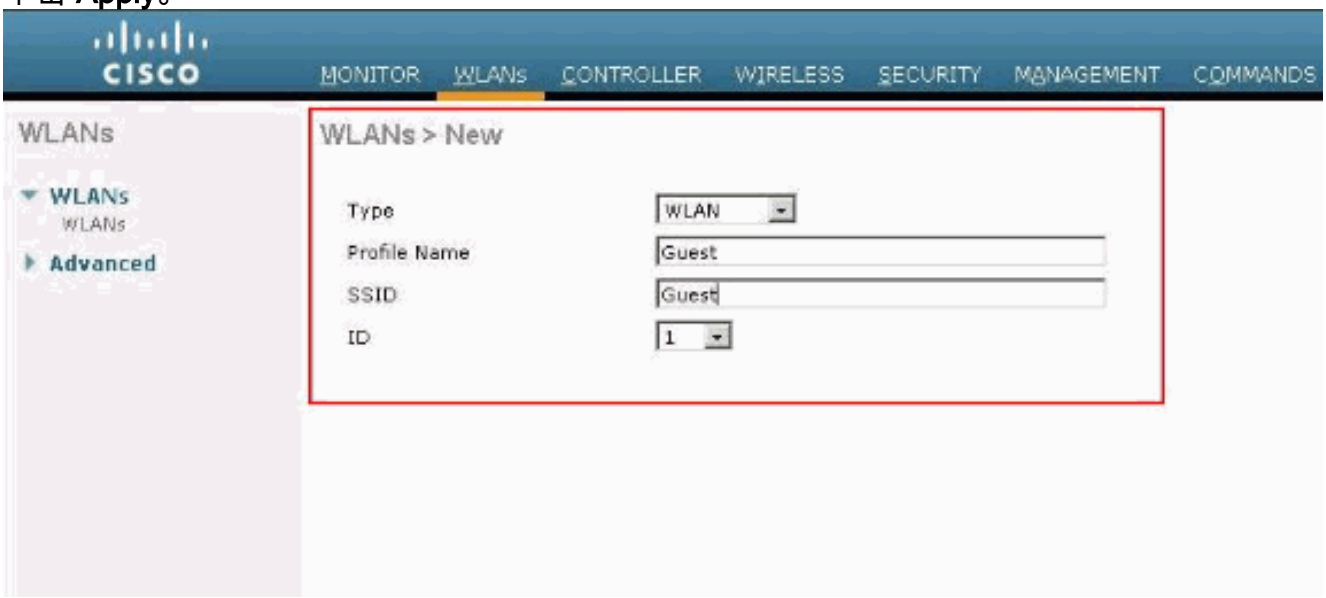


注意：在WLC版本5.0及更高版本中，也可以自定义Web身份验证的注销页面。有关如何配置它的详细信息，请参阅*无线LAN控制器配置指南5.2*的分配登录、登录失败和每个WLAN的注销页部分。

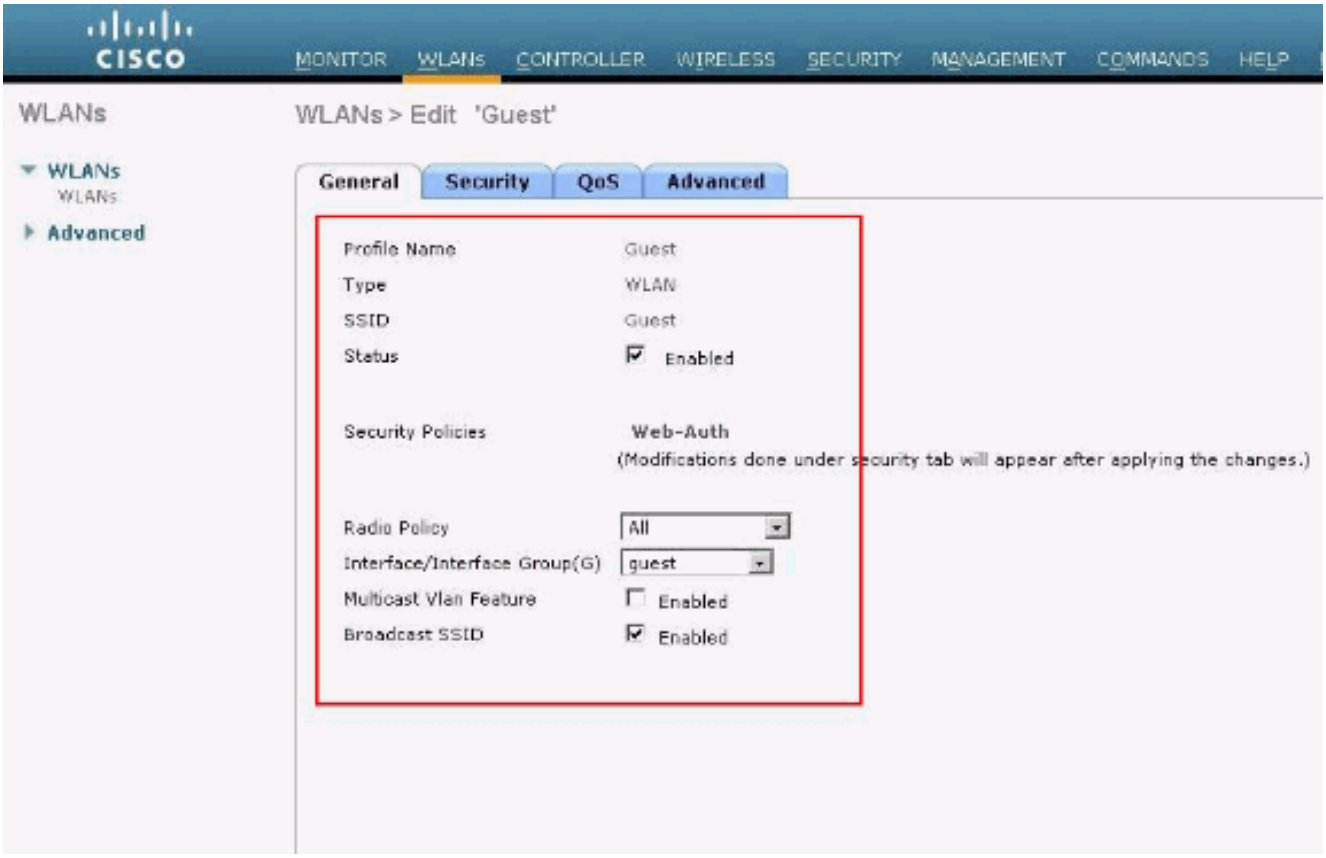
为来宾用户配置 WLAN

最后一步是为访客用户创建WLAN。请完成以下步骤：

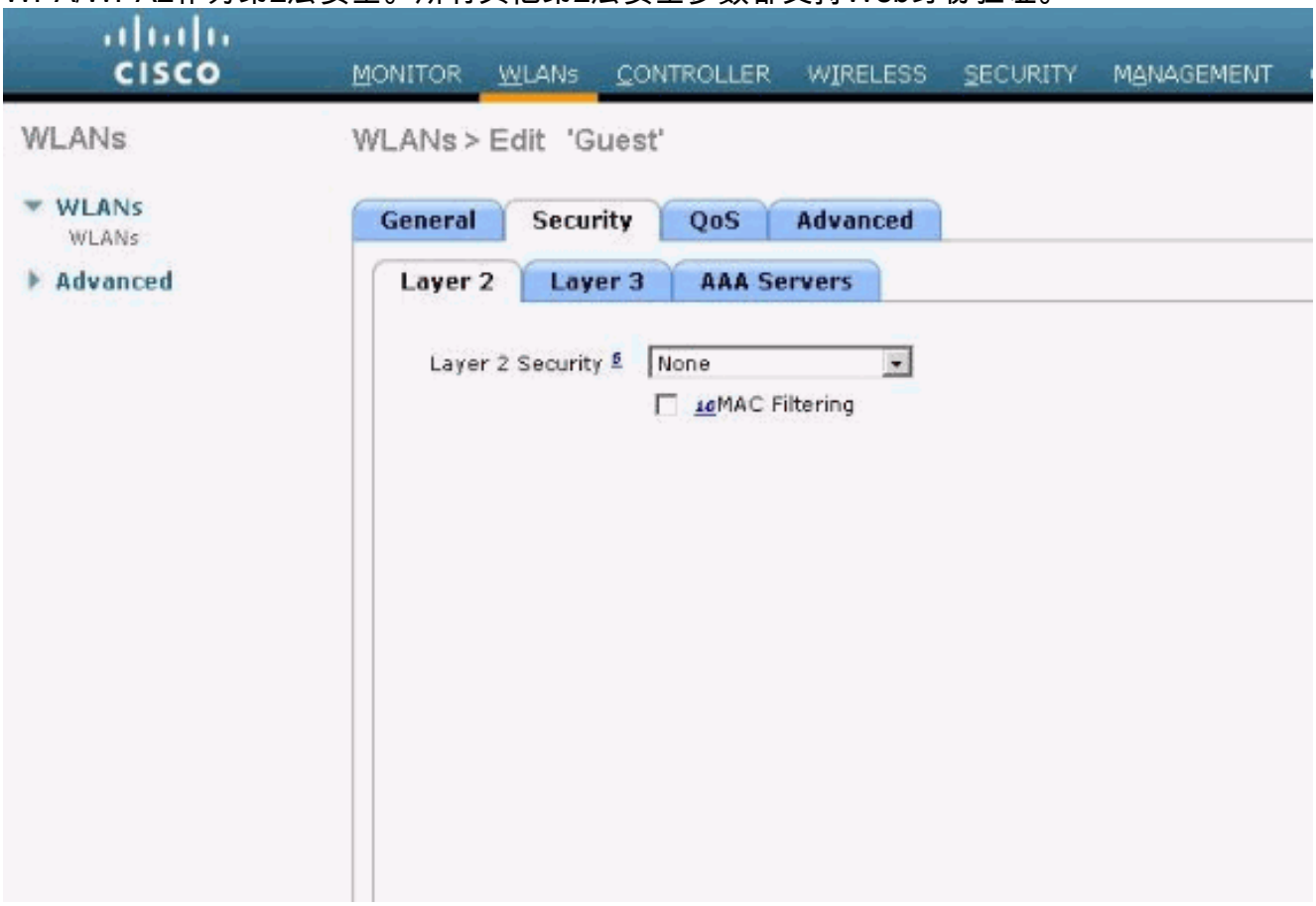
1. 要创建 WLAN，请从控制器 GUI 中单击 **WLANs**。随即显示 WLAN 窗口。该窗口列出了控制器中配置的 WLAN。
2. 要配置新的 WLAN，请单击 **New**。在本例中，WLAN 被命名为 **Guest，并且 WLAN ID 是 1**。
3. 单击 **Apply**。



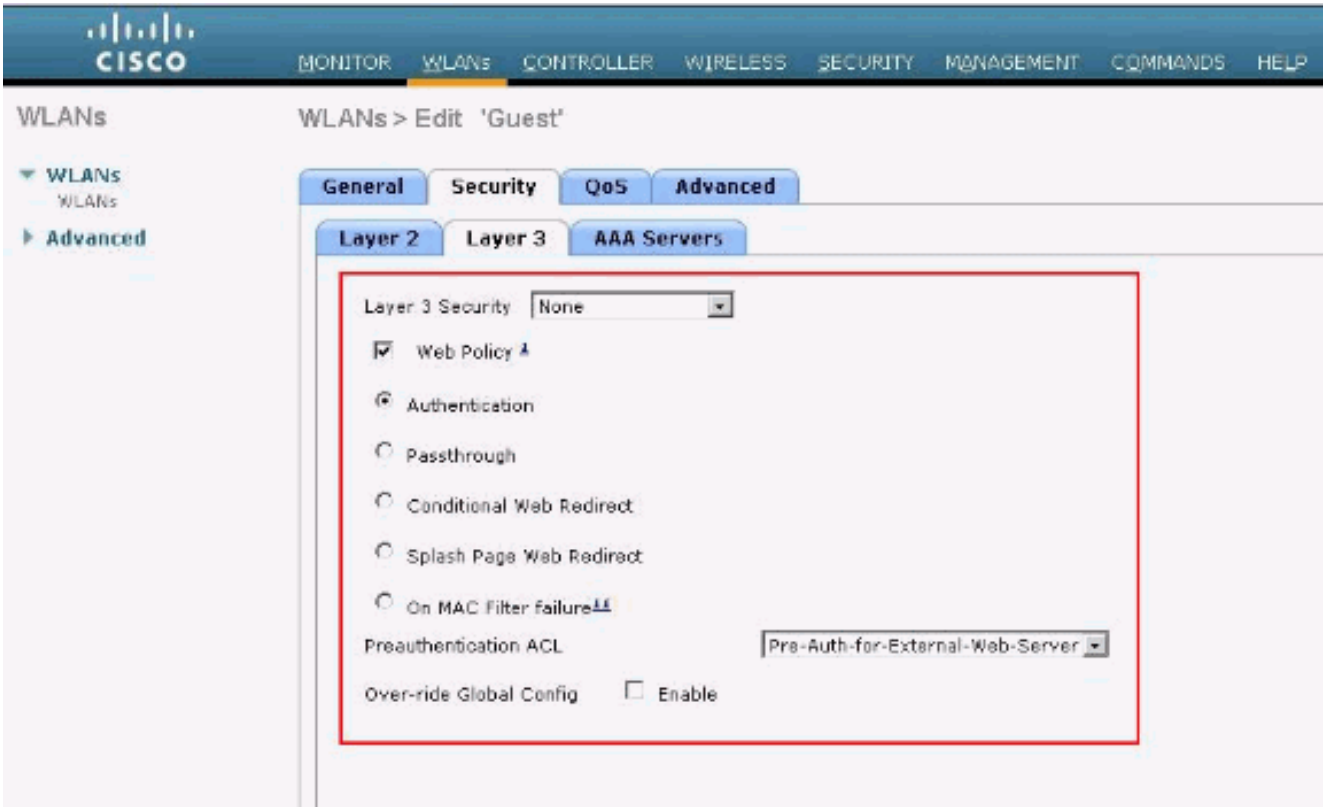
4. 在“WLAN”>“Edit”窗口中，定义特定于该 WLAN 的参数。对于访客WLAN，在General选项卡中，从Interface Name字段选择适当的接口。本示例将先前创建的动态接口 **guest 映射到 WLAN 来宾**。



转到安全选项卡。在本例中，在Layer 2 Security下选择**None**。**注意**：802.1x身份验证不支持Web身份验证。这意味着在使用Web身份验证时，不能选择802.1x或使用802.1x的WPA/WPA2作为第2层安全。所有其他第2层安全参数都支持Web身份验证。



在 Layer 3 Security 字段中，选中 **Web Policy 复选框并选择 Authentication 选项。**选择此选项是因为将使用 Web 身份验证对无线来宾客户端进行身份验证。从下拉菜单选择相应的预身份验证 ACL。在本例中，使用先前创建的预身份验证 ACL。单击 **Apply**。

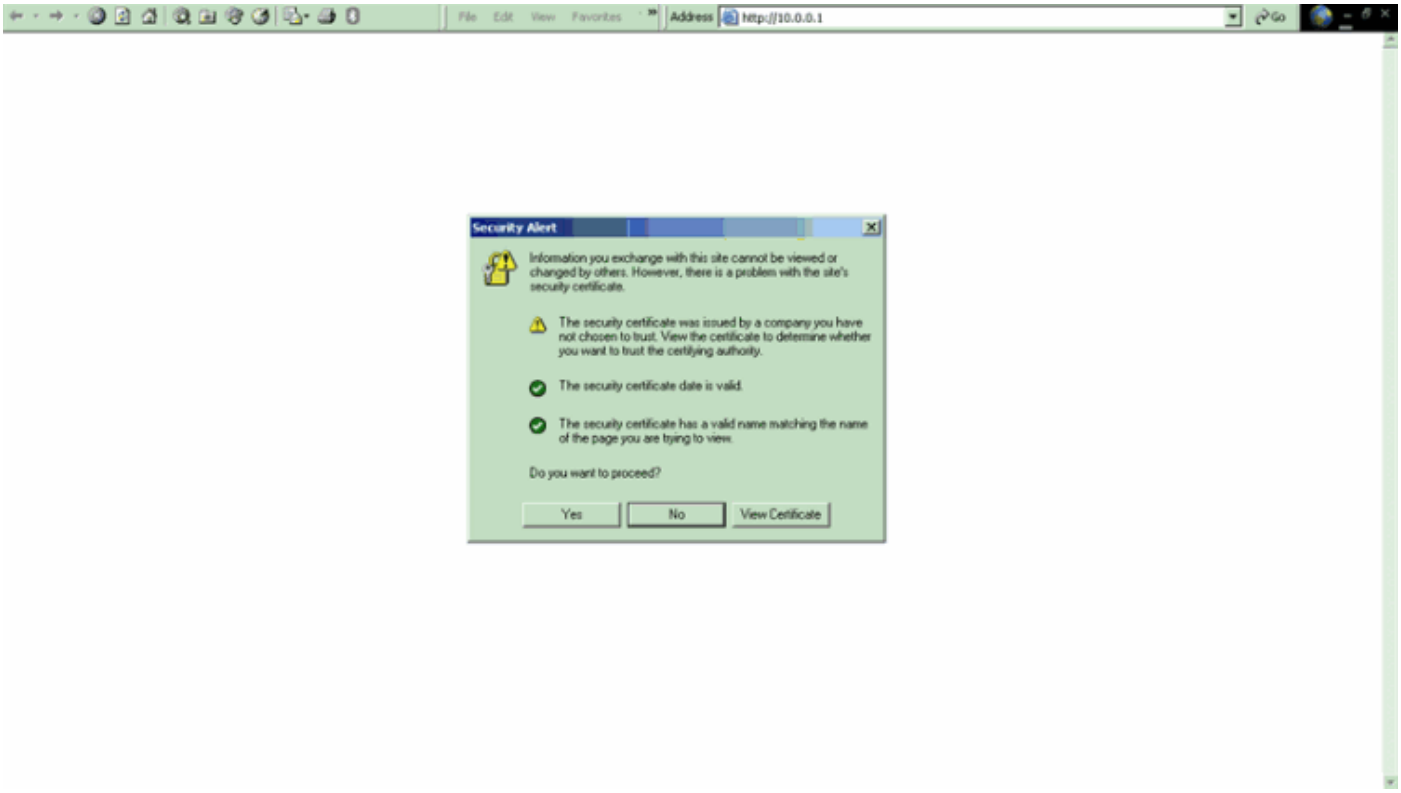


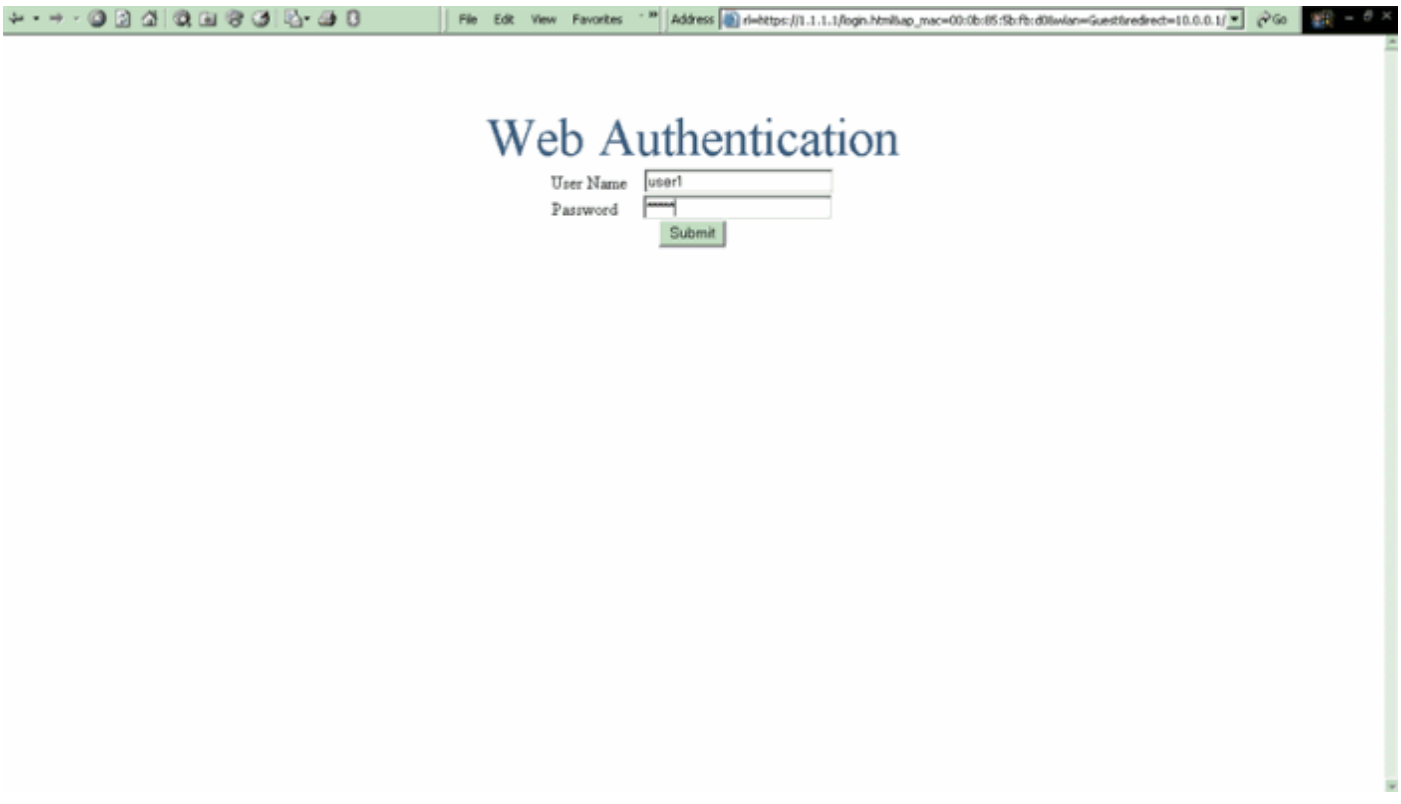
验证

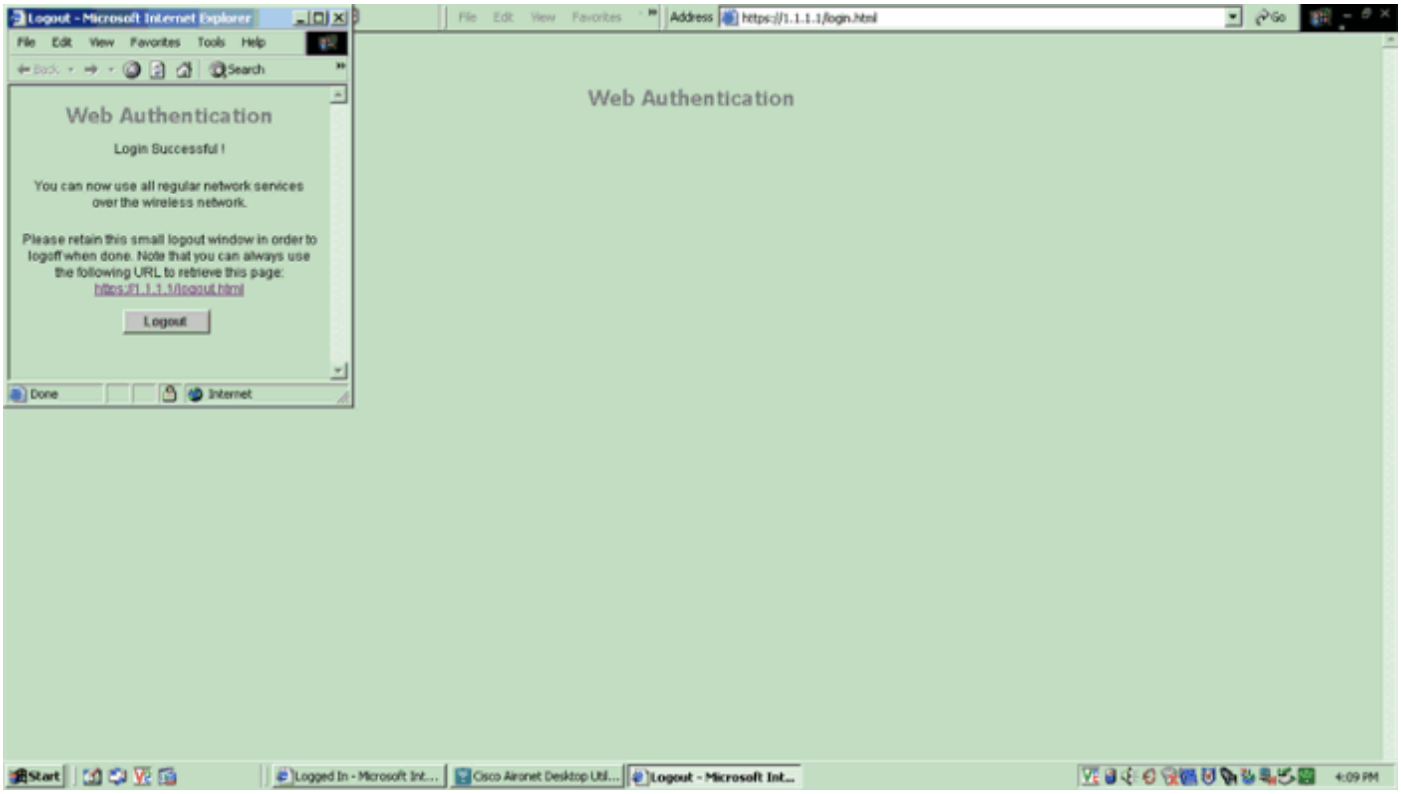
将会显示无线客户端，用户可以在 Web 浏览器中输入 URL（例如 www.cisco.com）。由于尚未对用户进行身份验证，因此，WLC 会将用户重定向到外部 Web 登录 URL。

将会提示用户输入用户凭证。一旦用户提交了用户名和口令，登录页将接收用户凭证输入，并在提交后将请求发送回 WLC Web 服务器的 action_URL（例如 http://1.1.1.1/login.html）。它以输入参数形式提供给客户重定向 URL，其中 1.1.1.1 是交换机上的虚拟接口地址。

WLC 将按照 WLC 上配置的本地数据库对用户进行身份验证。在成功进行身份验证后，WLC Web 服务器会将用户转送至已配置的重定向 URL 或客户端最初使用的 URL（例如 www.cisco.com）。


File Edit View Favorites
Address http://10.0.0.1
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The security certificate has a valid name matching the name of the page you are trying to view.
Do you want to proceed?
Yes
No
View Certificate


File Edit View Favorites
Address rl=https://1.1.1.1/login.html&ap_mac=00:0b:85:5b:fb:d0&wlan=Guest&redirect=10.0.0.1/
Web Authentication
User Name user1
Password
Submit



故障排除

使用下面这些调试命令可排除配置的故障。

- debug mac addr <client-MAC-address xx:xx:xx:xx:xx:xx>
- debug aaa all enable
- debug pem state enable
- debug pem events enable
- debug dhcp message enable
- debug dhcp packet enable
- debug pm ssh-appgw enable
- debug pm ssh-tcp enable

使用本部分可排除配置故障。

重定向到外部 Web 身份验证服务器的客户端收到证书警告

问题：当客户端重定向到思科的外部Web身份验证服务器时，它们会收到证书警告。服务器上有一个有效证书，如果您直接连接到外部 Web 身份验证服务器，则不会收到证书警告。这是否是因为 WLC 的虚拟 IP 地址 (1.1.1.1) 被提交给客户端而不是提交给与证书相关联的外部 Web 身份验证服务器的实际 IP 地址？

解决方案：是。不管您是执行本地 Web 身份验证还是外部 Web 身份验证，您都将在控制器上使用内部 Web 服务器。当您重定向到外部 Web 服务器时，您仍会从控制器收到证书警告，除非控制器上具有一个有效证书。如果重定向被发送到 https，您会收到来自控制器和外部 Web 服务器的证书警告，除非这两者都具有一个有效证书。

为了同时消除证书警告，您需要发布一个根级证书并下载到控制器上。该证书针对主机名进行发布，您需要在控制器上将该主机名放在虚拟接口下面的 DNS 主机名框中。您还需要将该主机名添加到您的本地 DNS 服务器，并使其指向 WLC 的虚拟 IP 地址 (1.1.1.1)。

有关详细信息，请参阅在WLAN控制器(WLC)上生成第三方证书的证书签名请求(CSR)。

错误："无法显示页面"

问题：将控制器升级到4.2.61.0后，当您使用下载的网页进行Web身份验证时，会出现"page cannot be displayed"错误消息。在升级之前，此操作可以顺利执行。默认的内部网页可以顺利加载而不出现任何问题。

解决方案：从WLC版本4.2及更高版本引入了一项新功能，其中可以有多个自定义登录页用于Web身份验证。

为了能够正确加载网页，在 Security > Web Auth > Web login page 中将 Web 身份验证类型全局设置为 **customized 并不足以解决问题。**还必须在特定的 WLAN 上进行配置。为此，请完成以下步骤：

1. 登录到 WLC 的 GUI。
2. 单击 **WLANs 选项卡，查看为进行 Web 身份验证而配置的 WLAN 的配置文件。**
3. 在 WLAN > Edit 页上，单击 **Security 选项卡。**然后，选择 **Layer 3。**
4. 在此页上，为 Layer 3 Security 选择 **None。**
5. 选中 **Web Policy 框，并选择 Authentication 选项。**
6. 选中 **Over-ride Global Config Enable 框，为 Web Auth Type 选择 Customized (Downloaded)，然后从 Login Page 下拉菜单中选择所需的登录页。**单击 **Apply。**

相关信息

- **无线局域网控制器 Web 身份验证配置示例**
- **视频：思科无线局域网控制器(WLC)上的Web身份验证**
- **无线局域网控制器上的 VLAN 配置示例**
- **无线 LAN 控制器和轻量接入点基本配置示例**
- **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）。