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

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[背景信息](#)
[配置](#)
[配置](#)
[WLC 配置](#)
[RADIUS 服务器配置](#)
[验证](#)
[故障排除](#)
[相关信息](#)

简介

本文解释包括的配置步骤验证无线局域网控制器(WLC)的大厅管理员用RADIUS服务器。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 知识如何配置在WLCs的基本参数
- 知识如何配置一个RADIUS服务器，例如Cisco Secure ACS
- 来宾用户知识WLC的

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科4400运行版本7.0.216.0的无线局域网控制器
- 运行软件版本4.1和使用作为RADIUS服务器在此配置方面的Cisco Secure ACS。

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

大厅管理员，亦称WLC的大厅大使，能创建和管理在无线局域网控制器(WLC)的来宾用户用户帐号。大厅大使有受限的配置权限，并且能访问用于的仅网页管理访客帐户。大厅大使能指定时间来宾用户用户帐号依然是活动。在指定的时间过去以后，来宾用户用户帐号自动地超时。

参考的部署指南：思科访客访问使用关于来宾用户的更多信息Cisco无线LAN控制器。

为了创建在WLC的一个来宾用户用户帐号，您需要登陆到控制器作为大厅管理员。本文解释用户如何验证到WLC，根据属性的大厅管理员由RADIUS服务器返回。

注意： 验证可能也执行的大厅管理员根据在WLC配置的本地大厅管理员帐户。参考创建一个大厅大使帐户对于信息如何创建大厅管理员帐户本地在控制器。

配置

在此部分，您提交与关于如何的信息配置WLC和Cisco Secure ACS在本文描述的目的。

配置

本文档使用以下配置：

- WLC的管理接口IP地址是10.77.244.212/27。
- RADIUS服务器的IP地址是10.77.244.197/27。
- 在接入点(AP)和RADIUS服务器使用的共享密钥是cisco123。
- 在RADIUS服务器配置的大厅管理员的用户名和密码是都lobbyadmin。

在本文的配置示例中，所有客户记录到有用户名和密码的控制器里作为lobbyadmin分配大厅管理员的角色。

WLC 配置

在您开始必要的WLC配置前，请保证您的控制器运行版本4.0.206.0或以上。这归结于Cisco Bug ID CSCsg89868 (仅限注册用户)控制器Web接口显示Lobbyadmin用户的错误的网页，当用户名在RADIUS数据库时存储。Lobbyadmin提交与只读接口而不是Lobbyadmin接口。

此bug在WLC版本4.0.206.0被解决了。所以，请保证您的控制器版本是4.0.206.0或以后。参考无线局域网控制器(WLC)软件升级关于关于如何的说明升级您的控制器到适当的版本。

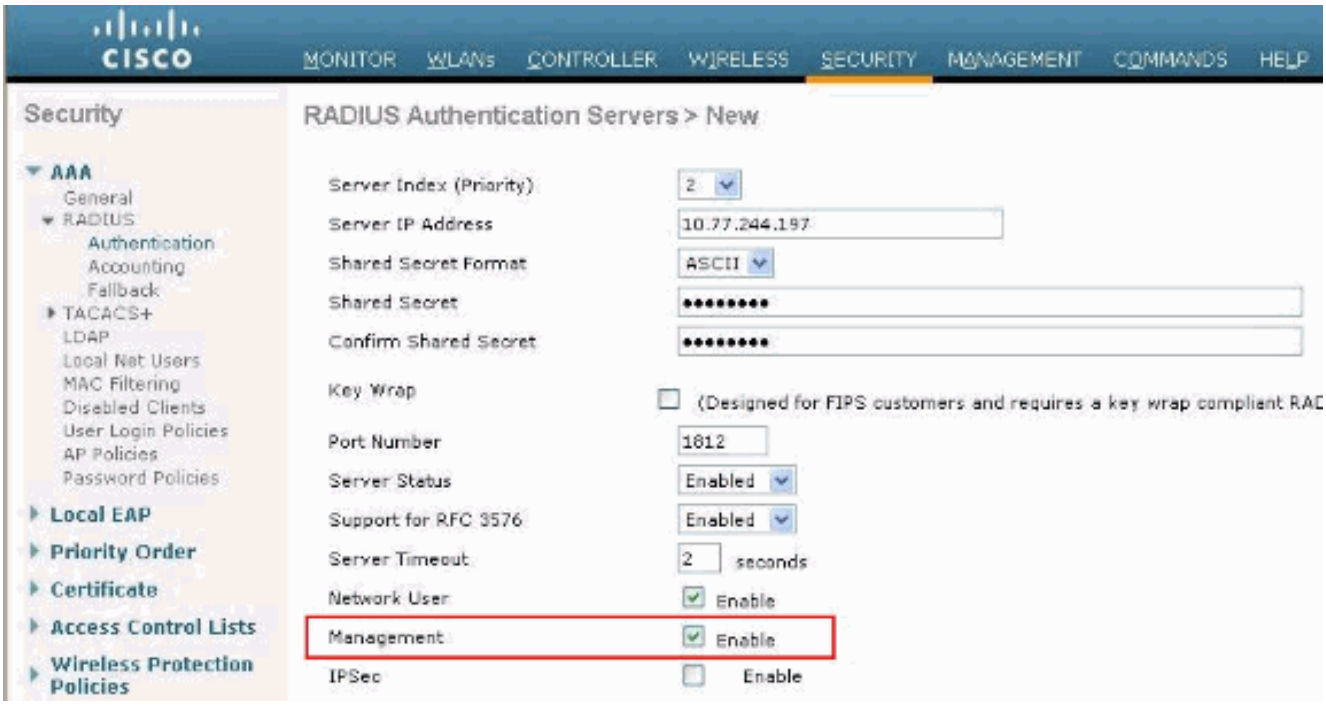
为了用RADIUS服务器执行控制器管理验证，请保证**Admin-auth-via-RADIUS**标志在控制器启用。这可以从**show radius summary命令**输出验证。

第一步将配置关于控制器的RADIUS服务器信息和设立在控制器和RADIUS服务器之间的第3层可接通性。

配置关于控制器的RADIUS服务器信息

完成这些步骤为了配置与详细信息的WLC关于ACS ：

1. 从WLC GUI，请选择**安全选项卡**并且配置ACS服务器的IP地址和共享机密。这共享秘密需要是相同的在ACS为了WLC能通信与ACS。**注意：** ACS共享的机密区分大小写。所以，请确保正确地输入共享秘密信息。此图显示示例
：



2. 如在step1的图所显示检查**管理**复选框为了允许ACS管理WLC用户。然后，单击 **Apply**。
3. 在**ping命令帮助下**验证在控制器和配置的RADIUS服务器之间的第3层可接通性。此ping选项也是可用的在配置的RADIUS服务器页在WLC GUI在**Security>RADIUS Authentication选项**。此图表显示从RADIUS服务器的一ping成功回复。所以，第3层可接通性是可用的在控制器和RADIUS服务器之间。

RADIUS 服务器配置

完成在这些部分的步骤为了配置RADIUS服务器：

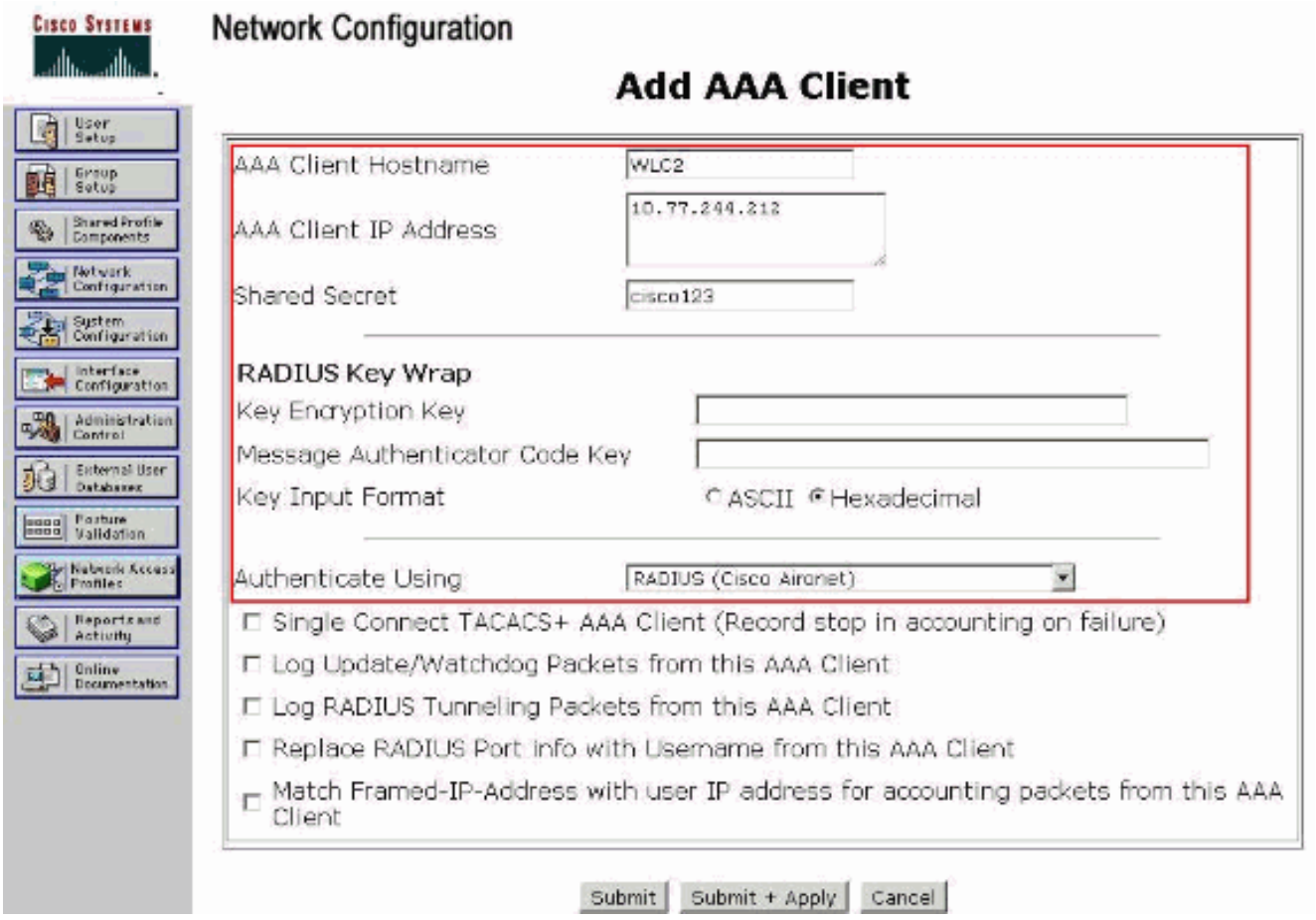
1. 添加WLC作为AAA客户端到RADIUS服务器
2. 配置大厅管理员的适当的RADIUS IETF类型属性

添加WLC作为AAA客户端到RADIUS服务器

完成这些步骤为了添加WLC作为RADIUS服务器的一个AAA客户端。如前面提到，本文使用ACS作为RADIUS服务器。您能使用所有RADIUS服务器此配置。

完成这些步骤为了添加WLC作为ACS的一个AAA客户端：

1. 从ACS GUI，请选择**Network Configuration选项**。
2. 在 AAA Clients 下，单击 **Add Entry**。
3. 在添加AAA客户端窗口，请输入WLC主机名、WLC的IP地址和共享密钥。请参阅示例图表在步骤5.下。
4. 从验证使用下拉菜单，请选择**RADIUS (Cisco Aironet)**。
5. 点击**Submit+Restart**为了保存配置。

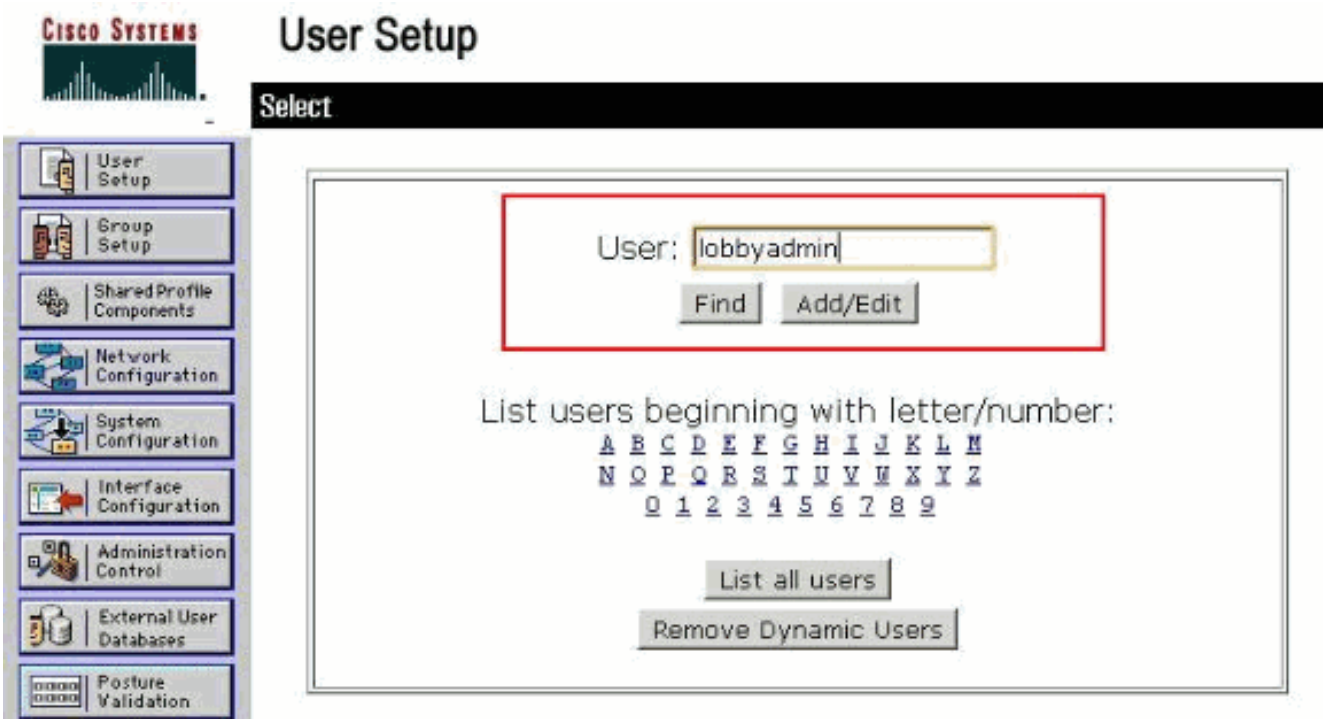


配置大厅管理员的适当的RADIUS IETF类型属性

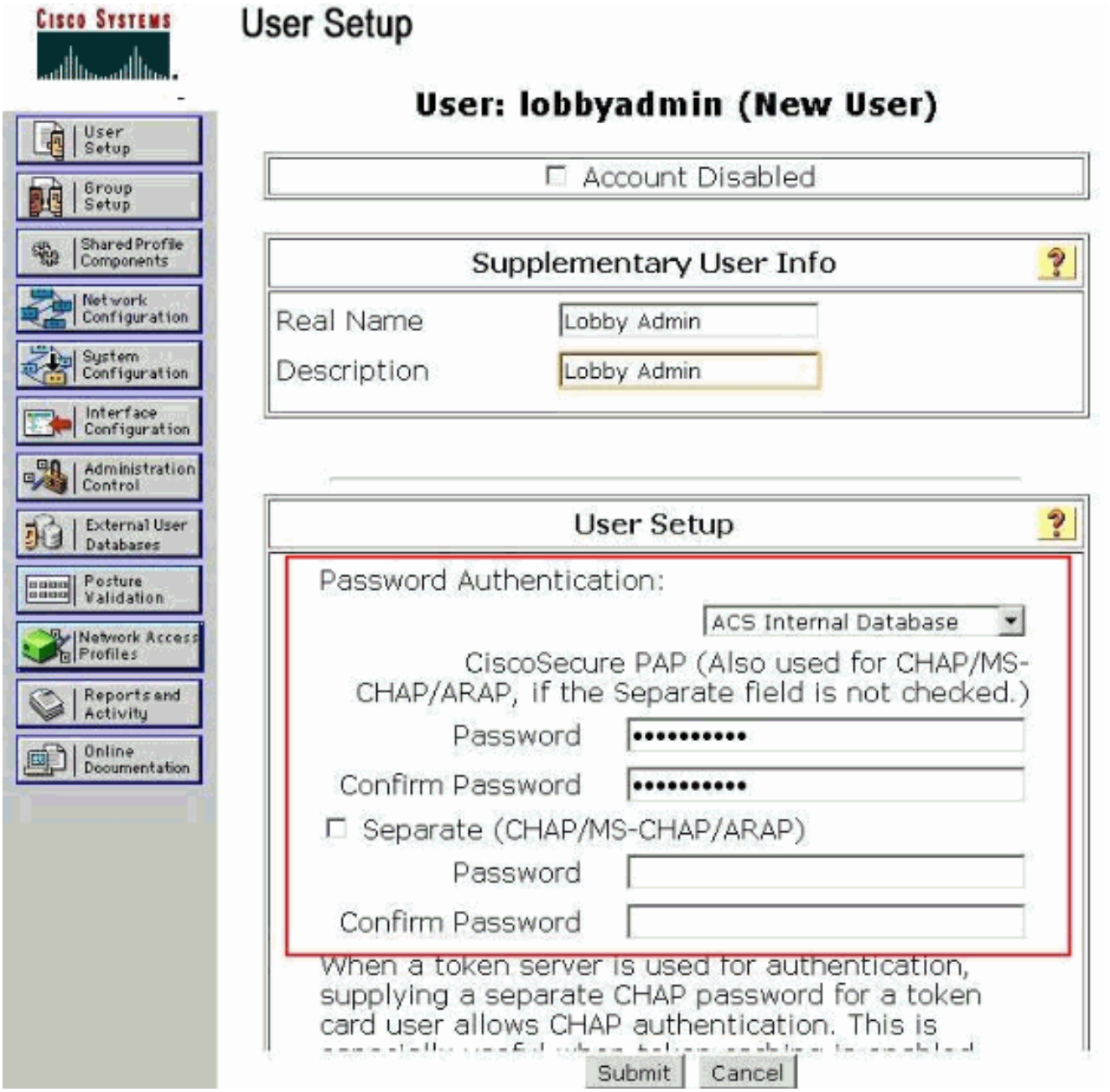
为了验证控制器的管理用户作为大厅管理员通过RADIUS服务器，您必须添加用户到RADIUS数据库IETF RADIUS服务类型属性设置为**管理的回拨**。此属性分配特定用户一个大厅管理员的角色控制器的。

本文显示用户lobbyadmin作为大厅管理员。为了配置此用户，请完成在ACS的这些步骤：

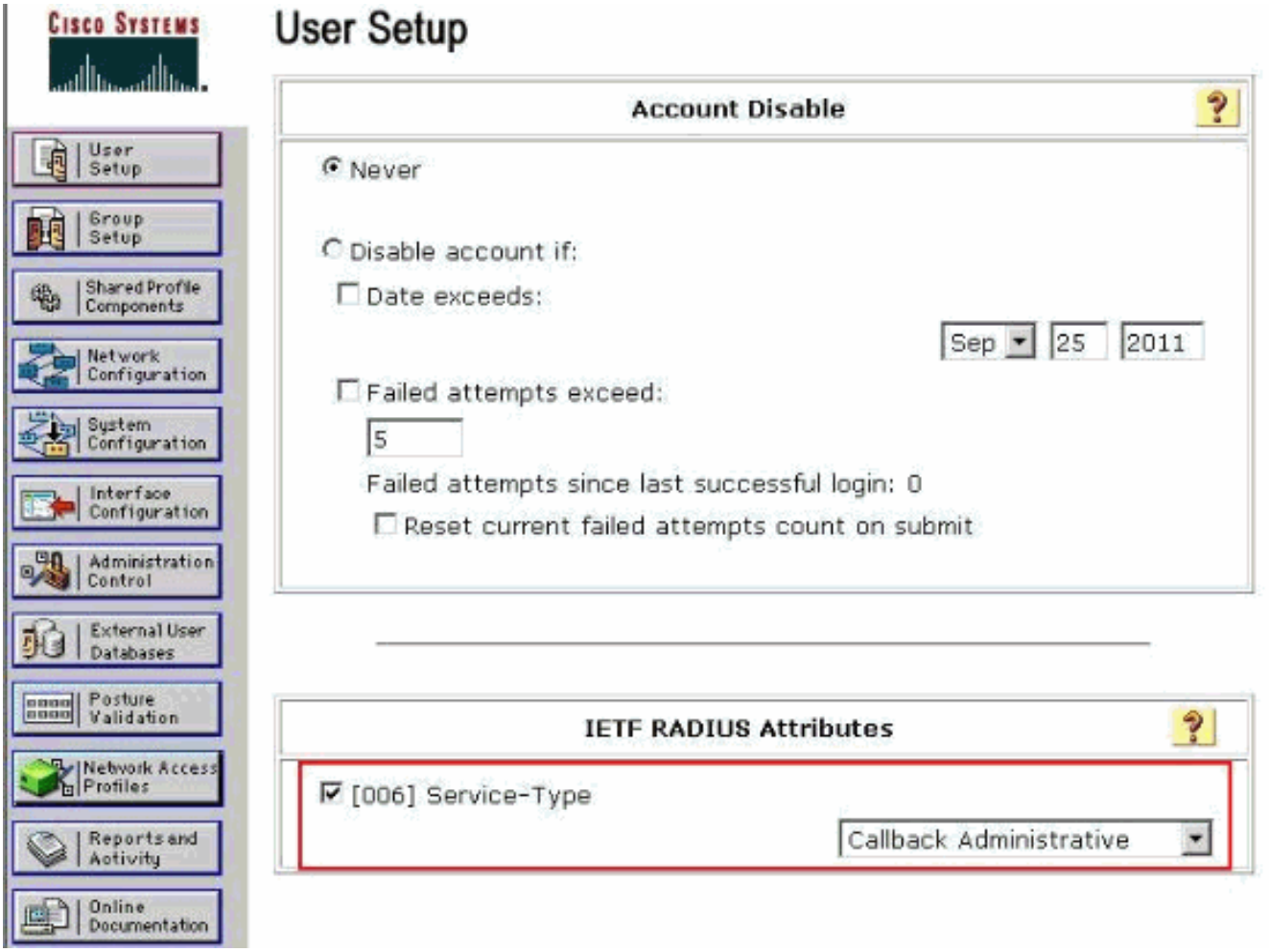
1. 从ACS GUI，请选择**User Setup选项**。
2. 输入将被添加的用户名到ACS，此示例窗口表示
   ：



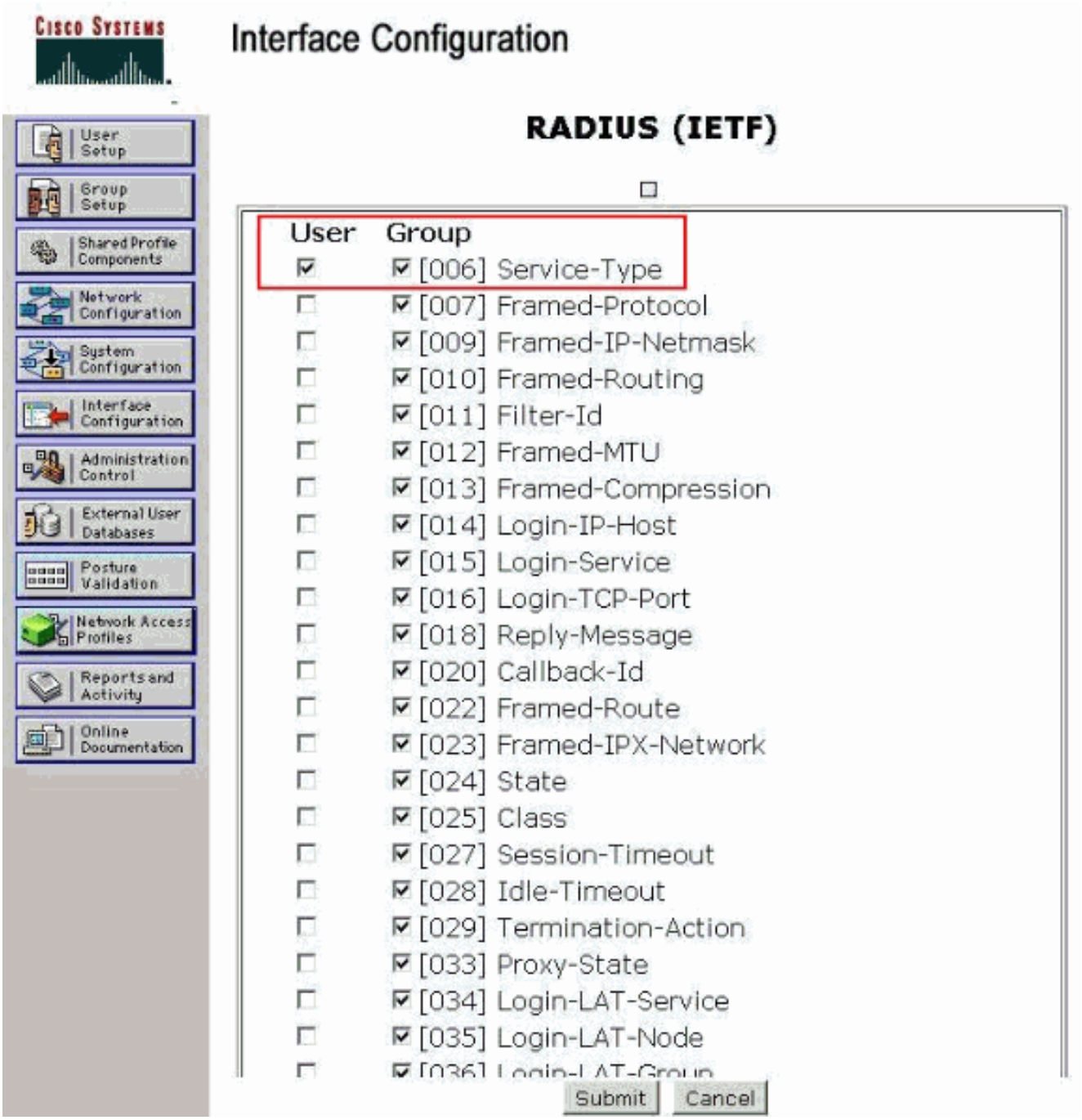
3. 单击**添加/编辑**为了去Edit页的用户。
4. 在Edit页的用户，请提供此用户真名、说明和密码细节。在本例中，使用的用户名和密码是都lobbyadmin。



5. 移下来对设置IETF的RADIUS属性并且检查**类型属性**复选框。
6. 从服务类型下拉菜单选择**管理的回拨**并且单击**提交**。这是分配此用户大厅管理员的角色的属性。



有时，此类型属性不是可视在用户设置下。在这类情况下，请完成这些步骤为了使可视：从ACS GUI，请选择**接口配置> RADIUS (IETF)**为了启用在用户配置窗口的IETF属性。这给Settings页的RADIUS (IETF)带来您。从Settings页的RADIUS (IETF)，您能启用需要是可视在用户或组设置下的IETF属性。对于此配置，请检查**服务类型**用户列并且单击**提交**。此窗口表示示例
：



注意： 此示例逐个用户指定验证。您可也执行根据特定用户属于的组的验证。在这类情况下，请检查**Group复选框，**以便此属性是可视在组设置下。**注意：** 并且，如果验证根据组基本类型，您需要分配用户给特定组并且配置组设置IETF属性提供访问权限给该组的用户。关于如何的参考的用户组管理配置与管理组的详细信息。

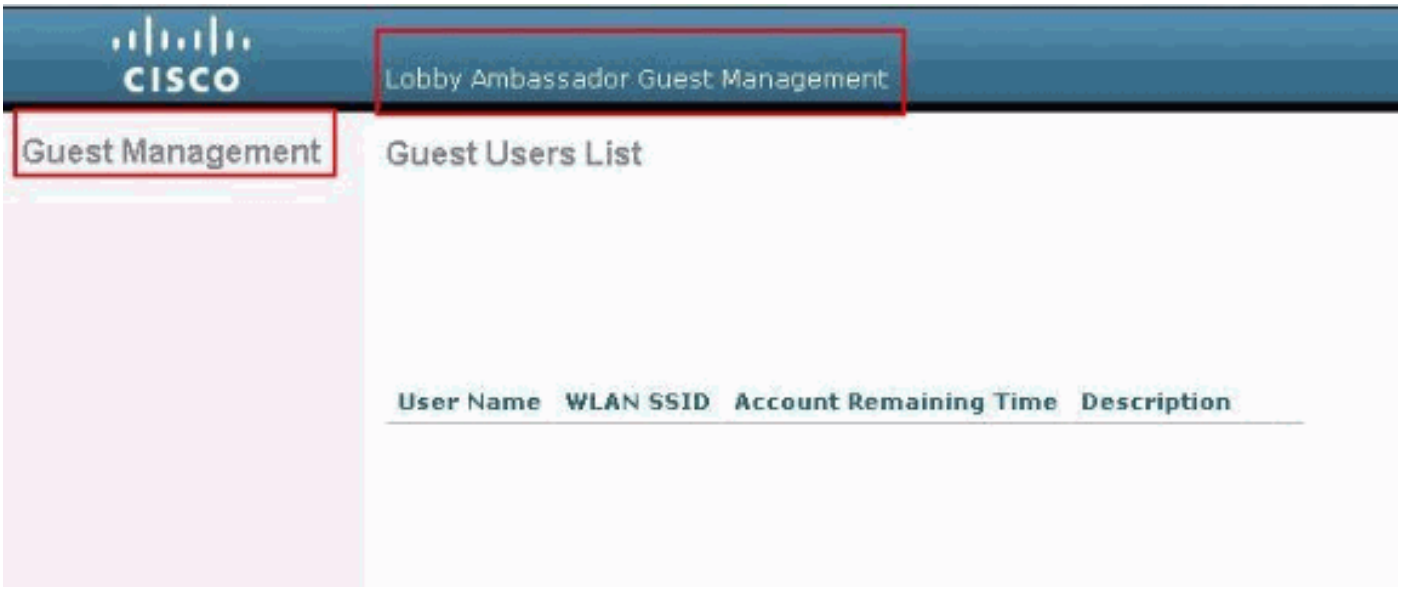
验证

使用本部分可确认配置能否正常运行。

为了验证您的配置适当地工作，请通过GUI (HTTP/HTTPS)模式访问WLC。

注意： 大使不访问控制器CLI接口并且的大厅能创建来宾用户仅用户帐号从控制器GUI。

当登录提示出现时，请输入用户名和密码如配置在ACS。如果有正确的配置，您顺利地验证到WLC作为**大厅管理员**。此示例显示大厅管理员的GUI如何照看成功认证：



注意： 您能看到除来宾用户管理外，大厅管理员没有其它选项。

为了从CLI模式验证它， Telnet到控制器作为一个读写管理员。发出**debug aaa all enable命令**在控制器CLI。

```
(Cisco Controller) >debug aaa all enable (Cisco Controller) > *aaaQueueReader: Aug 26
18:07:35.072: ReProcessAuthentication previous proto 28, next proto 20001 *aaaQueueReader: Aug
26 18:07:35.072: AuthenticationRequest: 0x3081f7dc *aaaQueueReader: Aug 26 18:07:35.072:
Callback.....................................0x10756dd0 *aaaQueueReader: Aug 26 18:07:35.072:
protocolType.................................0x00020001 *aaaQueueReader: Aug 26 18:07:35.072:
proxyState...................................00:00:00:40: 00:00-00:00 *aaaQueueReader: Aug 26
18:07:35.072: Packet contains 5 AVPs (not shown) *aaaQueueReader: Aug 26 18:07:35.072:
apfVapRadiusInfoGet: WLAN(0) dynamic int attributes srcAddr: 0x0, gw:0x0, mask:0x0, vlan:0,
dpPort:0, srcPort:0 *aaaQueueReader: Aug 26 18:07:35.073: 00:00:00:40:00:00 Successful
transmission of Authentication Packet (id 39) to 10.77.244.212:1812, proxy state
00:00:00:40:00:00-00:01 *aaaQueueReader: Aug 26 18:07:35.073: 00000000: 01 27 00 47 00 00 00 00
00 00 00 00 00 00 00 00 .'.G............ *aaaQueueReader: Aug 26 18:07:35.073: 00000010: 00 00
00 00 01 0c 6c 6f 62 62 79 61 64 6d 69 6e ......lobbyadmin *aaaQueueReader: Aug 26 18:07:35.073:
00000020: 02 12 5f 5b 5c 12 c5 c8 52 d3 3f 4f 4f 8e 9d 38 .._[\...R.?OO..8 *aaaQueueReader: Aug
26 18:07:35.073: 00000030: 42 91 06 06 00 00 00 07 04 06 0a 4e b1 1a 20 09 B..........N....
*aaaQueueReader: Aug 26 18:07:35.073: 00000040: 57 4c 43 34 34 30 30 WLC4400
*radiusTransportThread: Aug 26 18:07:35.080: 00000000: 02 27 00 40 7e 04 6d 533d ed 79 9c b6 99
d1 f8 .'.@~.mS=.y..... *radiusTransportThread: Aug 26 18:07:35.080: 00000010: d0 5a 8f 4f 08 06
ff ffff ff 06 06 00 00 00 0b .Z.O............ *radiusTransportThread: Aug 26 18:07:35.080:
00000020: 19 20 43 41 43 53 3a 302f 61 65 32 36 2f 61 34 ..CACS:0/ae26/a4
*radiusTransportThread: Aug 26 18:07:35.080: 00000030: 65 62 31 31 61 2f 6c 6f62 62 79 61 64 6d
69 6e eb11a/lobbyadmin *radiusTransportThread: Aug 26 18:07:35.080: ****Enter
processIncomingMessages: response code=2 *radiusTransportThread: Aug 26 18:07:35.080: ****Enter
processRadiusResponse: response code=2 *radiusTransportThread: Aug 26 18:07:35.080:
00:00:00:40:00:00 Access-Accept received from RADIUS server 10.77.244.212 for mobile
00:00:00:40:00:00 receiveId = 0 *radiusTransportThread: Aug 26 18:07:35.080:
AuthorizationResponse: 0x13c73d50 *radiusTransportThread: Aug 26 18:07:35.080:
structureSize................................118 *radiusTransportThread: Aug 26 18:07:35.080:
resultCode...................................0 *radiusTransportThread: Aug 26 18:07:35.080:
protocolUsed.................................0x00000001 *radiusTransportThread: Aug 26
18:07:35.080: proxyState.....................................00:00:00:40:00:00-00:00
*radiusTransportThread: Aug 26 18:07:35.080: Packet contains 3 AVPs: *radiusTransportThread: Aug
26 18:07:35.080: AVP[01] Framed-IP-Address.....................0xffffffff (-1) (4 bytes)
*radiusTransportThread: Aug 26 18:07:35.080: AVP[02] Service-
Type.............................0x0000000b (11) (4 bytes) *radiusTransportThread: Aug 26
18:07:35.080: AVP[03] Class..................................... CACS:0/ae26/a4eb11a/lobbyadmin
(30 bytes) *emWeb: Aug 26 18:07:35.084: Authentication succeeded for lobbyadmin
```

在选中项目信息在此输出中，您能看到类型属性11 (管理的回拨)通过在从ACS服务器和用户的控制

器上登陆作为大厅管理员。

这些命令也许是另外的帮助：

- debug aaa详细信息enable (event)
- debug aaa events enable
- debug aaa packets enable

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

故障排除

当您登陆到一个控制器有大厅大使权限时，您不能创建与"**0**"生命时间时间值的一个来宾用户用户帐号，是帐户从未超时。在这些情况下，您收到0错误消息。

这归结于Cisco Bug ID CSCsf32392 (仅限注册用户)，找到主要与WLC版本4.0。此bug在WLC版本4.1被解决了。

相关信息

- 控制器上的管理用户的RADIUS服务器认证配置示例
- Cisco统一无线网络TACACS+配置
- Cisco无线LAN控制器配置指南，版本4.0 -管理用户帐户
- 无线 LAN 控制器中的 ACL 配置示例
- 无线局域网控制器(WLC)常见问题
- 在无线局域网控制器的ACL ：规则、限制和示例
- 使用无线局域网控制器的外部 Web 身份验证配置示例
- 无线局域网控制器 Web 身份验证配置示例
- 使用 WLC 的访客 WLAN 和内部 WLAN 配置示例
- 技术支持和文档 - Cisco Systems