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

本文档说明了使用RADIUS服务器对无线局域网控制器(WLC)的大厅管理员进行身份验证所涉及的配置步骤。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 了解如何在WLC上配置基本参数
- 了解如何配置RADIUS服务器，例如Cisco Secure ACS
- WLC中访客用户的知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行版本7.0.216.0的Cisco 4400无线LAN控制器
- 运行软件版本4.1并用作此配置中RADIUS服务器的思科安全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（也称为WLC的大厅大使）可以在无线LAN控制器(WLC)上创建和管理访客用户帐户。大厅大使具有有限的配置权限，只能访问用于管理访客帐户的网页。大厅大使可以指定访客用户帐户保持活动状态的时间。经过指定时间后，访客用户帐户将自动过期。

请参阅《部署指南》：使用思科无线局域网控制器的思科访客接入，了解有关访客用户的详细信息。

要在WLC上创建访客用户帐户，您需要以接待管理员的身份登录控制器。本文档说明如何根据RADIUS服务器返回的属性将用户作为大厅管理员身份验证到WLC中。

注意：也可以根据在WLC上本地配置的大厅管理员帐户执行大厅管理员身份验证。有关如何在控制器上本地创建大厅管理员帐户的信息，请参阅创建大厅大使帐户。

配置

在本节中，您将获得有关如何配置WLC和Cisco Secure ACS的信息，以实现本文档中所述的目的。

配置

本文档使用以下配置：

- WLC的管理接口IP地址为10.77.244.212/27。
- RADIUS服务器的IP地址为10.77.244.197/27。
- 在接入点(AP)和RADIUS服务器上使用的共享密钥是cisco123。
- 在RADIUS服务器中配置的大厅管理员的用户名和密码均为lobbyadmin。

在本文档的配置示例中，任何以用户名和密码为lobbyadmin登录控制器的用户都被分配接待管理员的角色。

WLC 配置

在开始必要的WLC配置之前，请确保您的控制器运行版本4.0.206.0或更高版本。这是由于Cisco Bug ID CSCsg89868 (仅限注册客户)，当用户名存储在RADIUS数据库中时，控制器的Web界面显示LobbyAdmin用户的错误网页。LobbyAdmin显示ReadOnly接口，而不是LobbyAdmin接口。

WLC版本4.0.206.0中已解决此Bug。因此，请确保您的控制器版本为4.0.206.0或更高版本。有关如何将控制器升级到相应版本的说明，请参阅无线LAN控制器(WLC)软件升级。

要使用RADIUS服务器执行控制器管理身份验证，请确保在控制器上启用**Admin-auth-via-RADIUS**标志。这可以从show radius summary命**令输出**中验证。

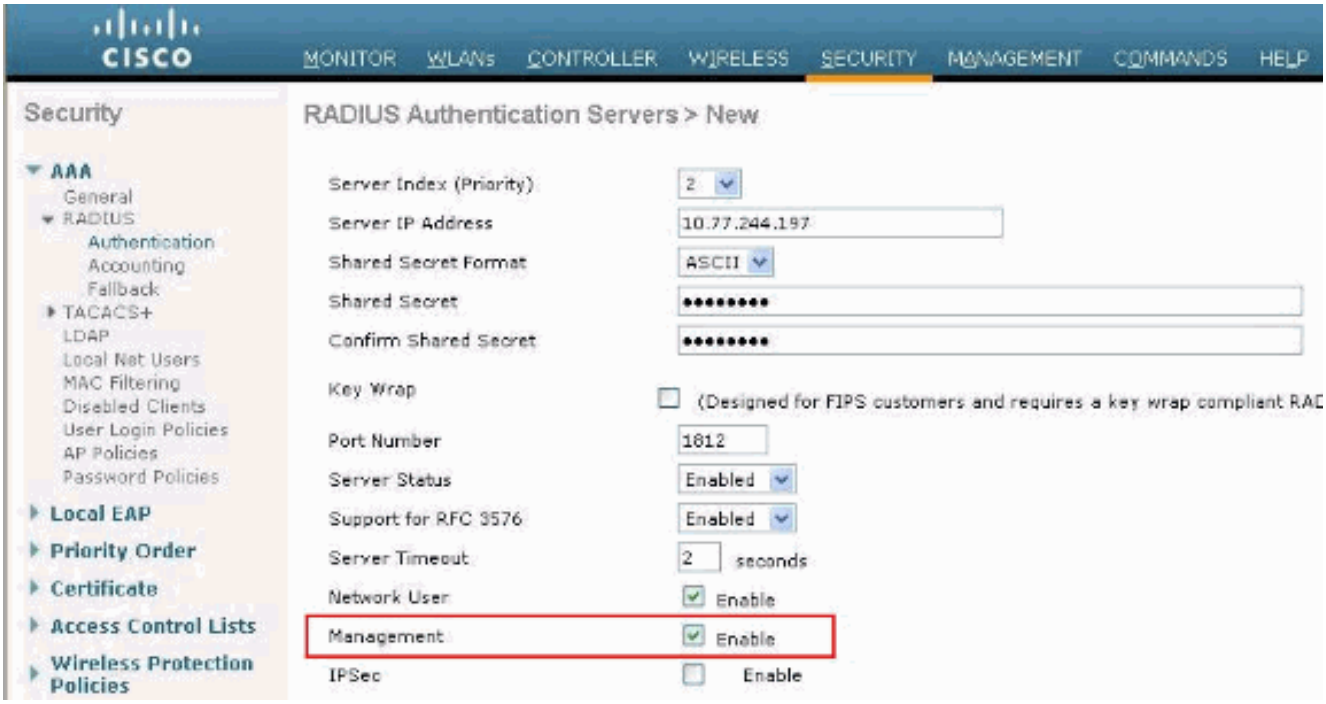
第一步是在控制器上配置RADIUS服务器信息，并在控制器和RADIUS服务器之间建立第3层可达性

。

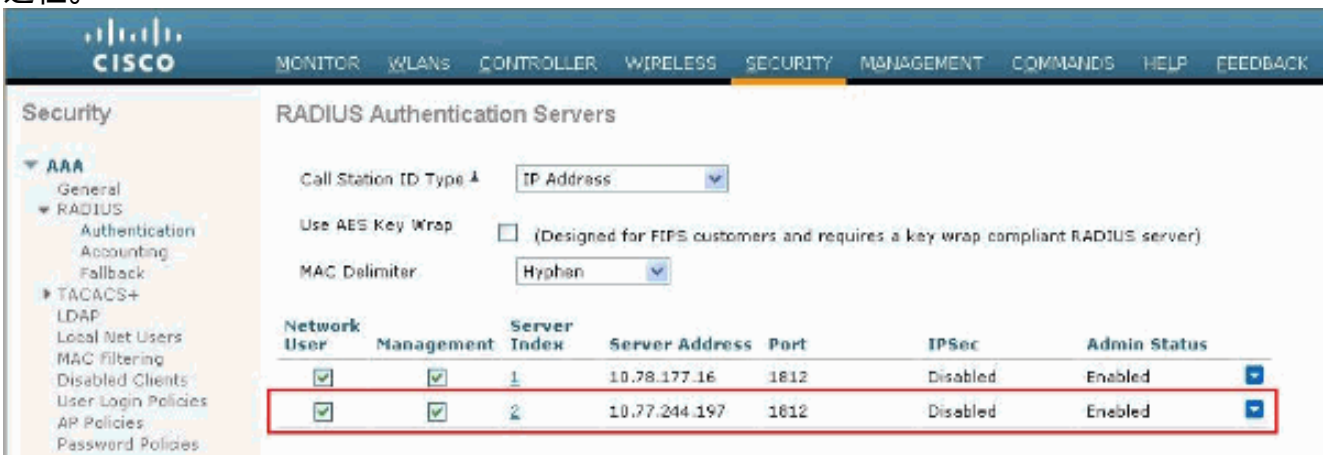
在控制器上配置RADIUS服务器信息

要配置WLC，请完成以下步骤，提供有关ACS的详细信息：

1. 从WLC GUI中，选择**Security**选项卡并配置ACS服务器的IP地址和共享密钥。ACS上的此共享密钥必须相同，WLC才能与ACS通信。**注意：** ACS共享密钥区分大小写。因此，请确保正确输入共享密钥信息。此图显示了一个示例
：



2. 如步骤1中的图所示，选中**Management**复选框以允许ACS管理WLC用户。然后单击**Apply**。
3. 借助**ping**命令验证控制器与已配置的RADIUS服务器之间的第3层可达性。此ping选项也可在WLC GUI的已配置RADIUS服务器页面的Security>RADIUS Authentication**选项卡中**使用。此图显示从RADIUS服务器成功执行ping应答。因此，控制器和RADIUS服务器之间具有第3层可达性。



RADIUS 服务器配置

要配置RADIUS服务器，请完成以下各节中的步骤：

1. 将WLC作为AAA客户端添加到RADIUS服务器

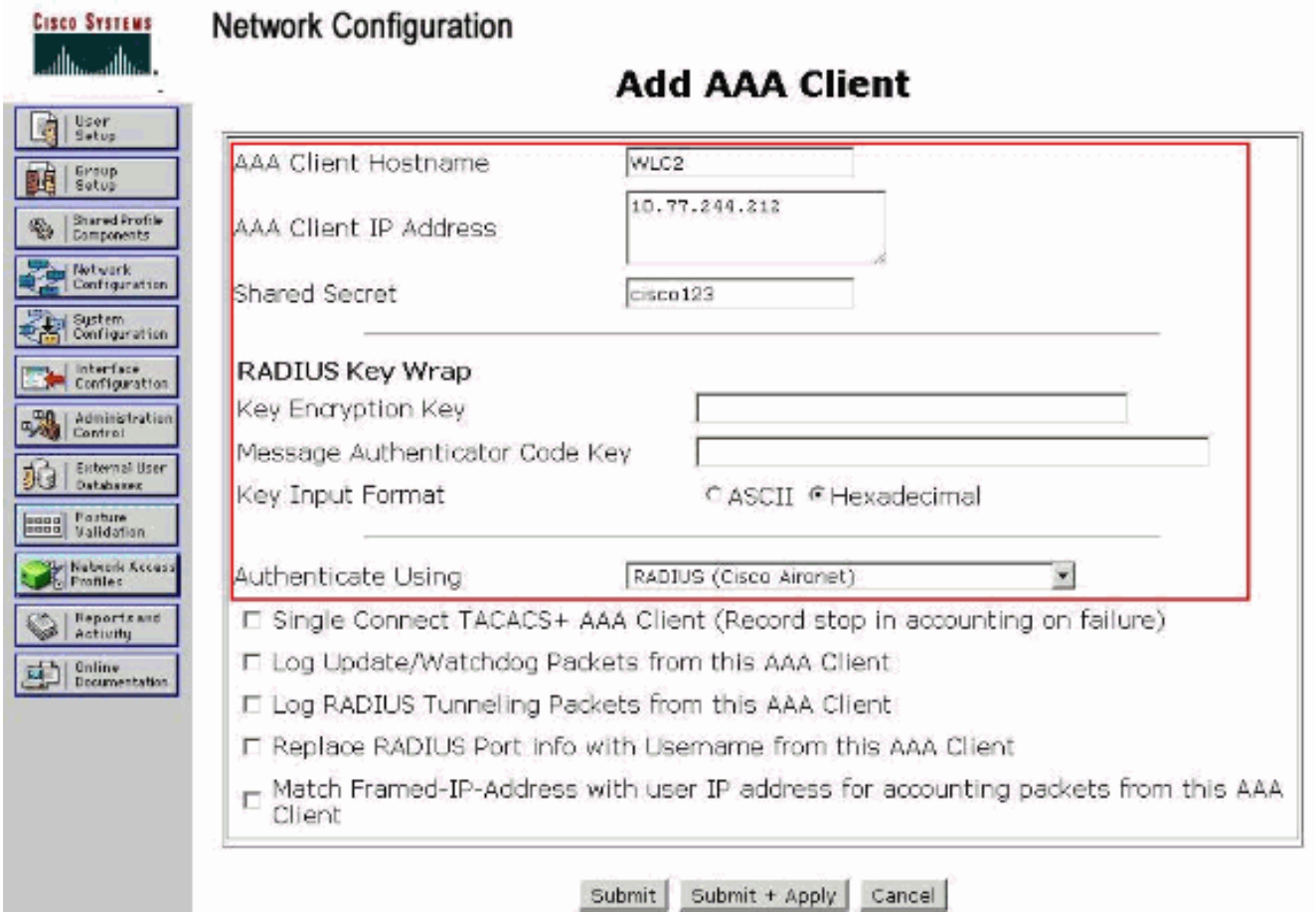
2. 为大厅管理员配置适当的RADIUS IETF服务类型属性

将WLC作为AAA客户端添加到RADIUS服务器

要将WLC添加为RADIUS服务器中的AAA客户端，请完成以下步骤。如前所述，本文档使用ACS作为RADIUS服务器。您可以使用任何RADIUS服务器进行此配置。

要在ACS中将WLC添加为AAA客户端，请完成以下步骤：

1. 从ACS GUI中，选择Network Configuration(**网络配置**)选项卡。
2. 在 AAA Clients 下，单击 **Add Entry**。
3. 在Add AAA Client（添加AAA客户端）窗口中，输入WLC主机名、WLC的IP地址和共享密钥。请参阅步骤5下的示例图。
4. 从Authenticate Using下拉菜单中，选择**RADIUS(Cisco Aironet)**。
5. 单击**Submit + Restart**以保存配置。

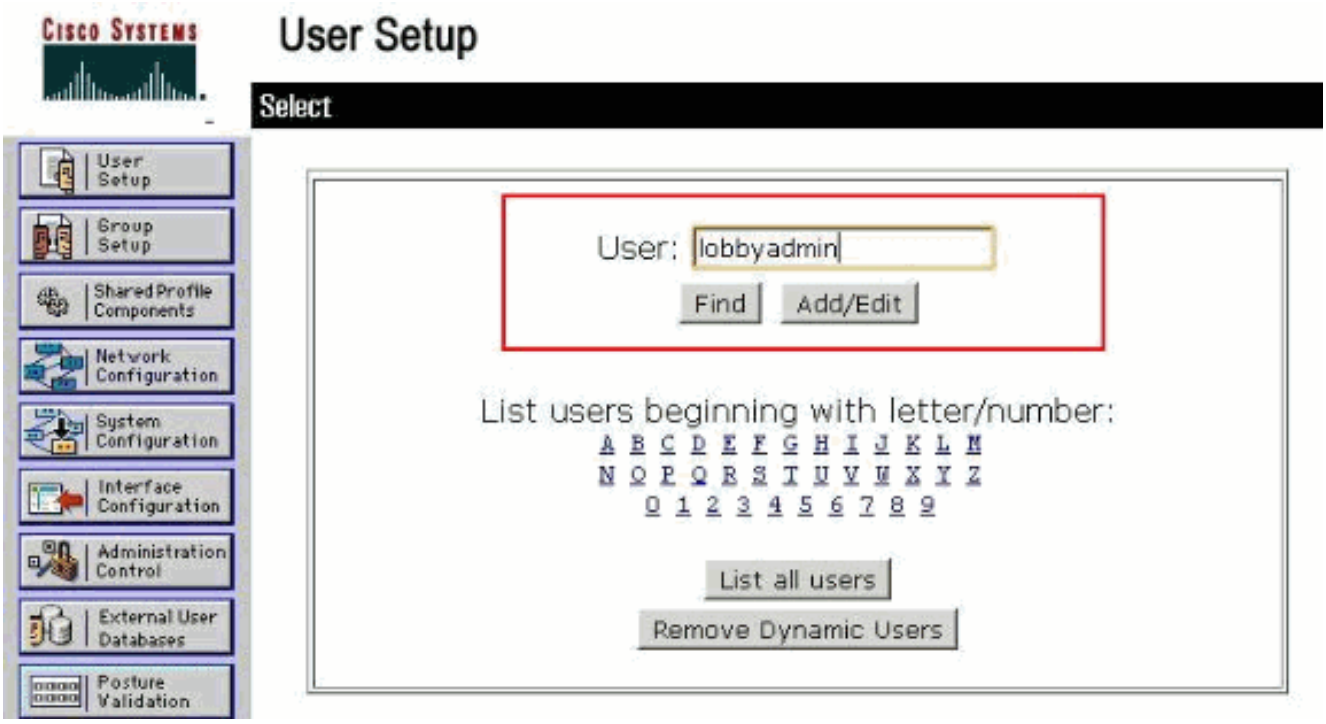


为大厅管理员配置适当的RADIUS IETF服务类型属性

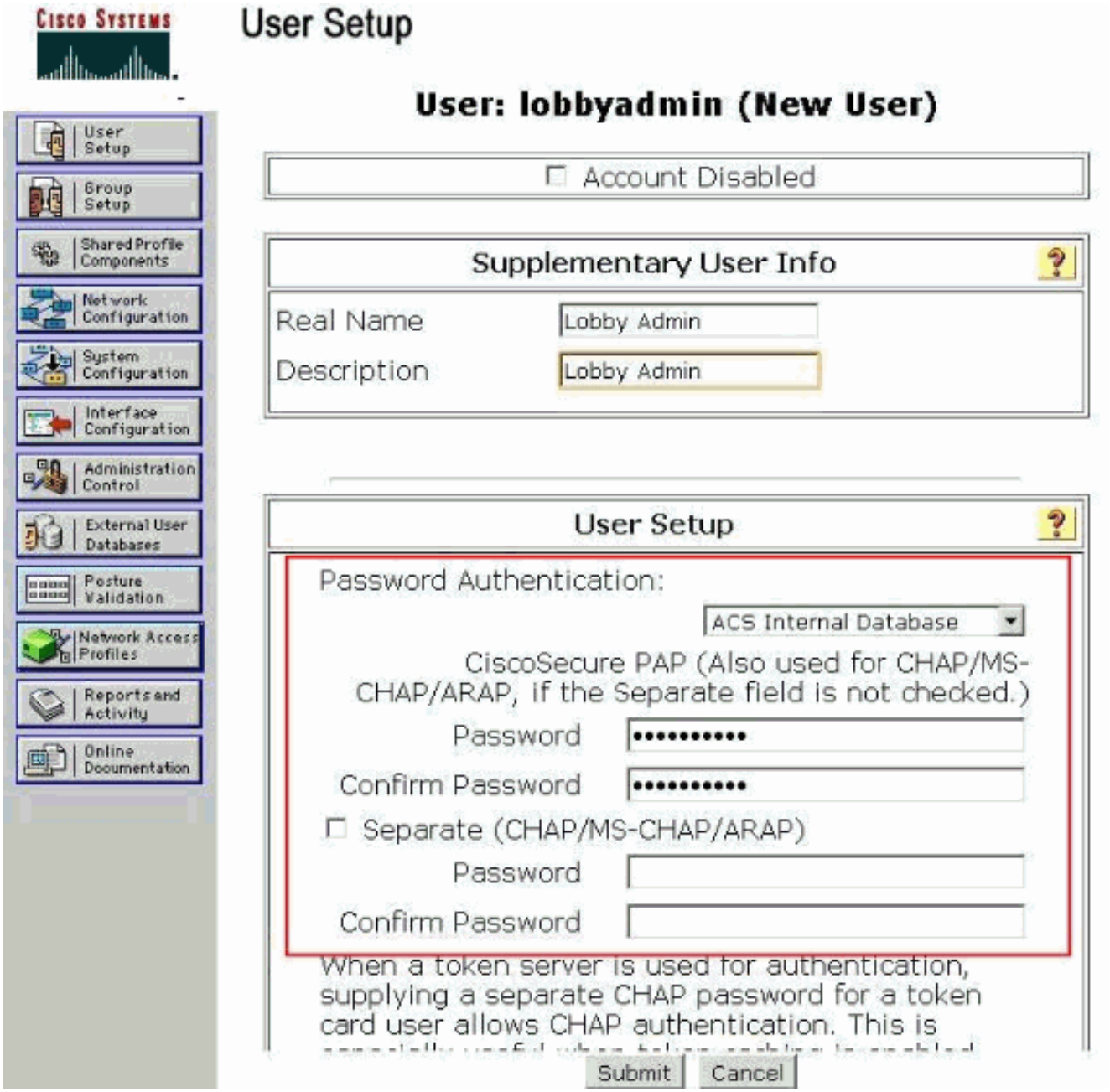
要通过RADIUS服务器将控制器的管理用户作为大厅管理员进行身份验证，必须将该用户添加到RADIUS数据库，并将IETF RADIUS Service-Type属性设置为“回叫管理”。此属性为特定用户分配控制器上大厅管理员的角色。

本文档显示作为大厅管理员的示例用户lobbyadmin。要配置此用户，请在ACS上完成以下步骤：

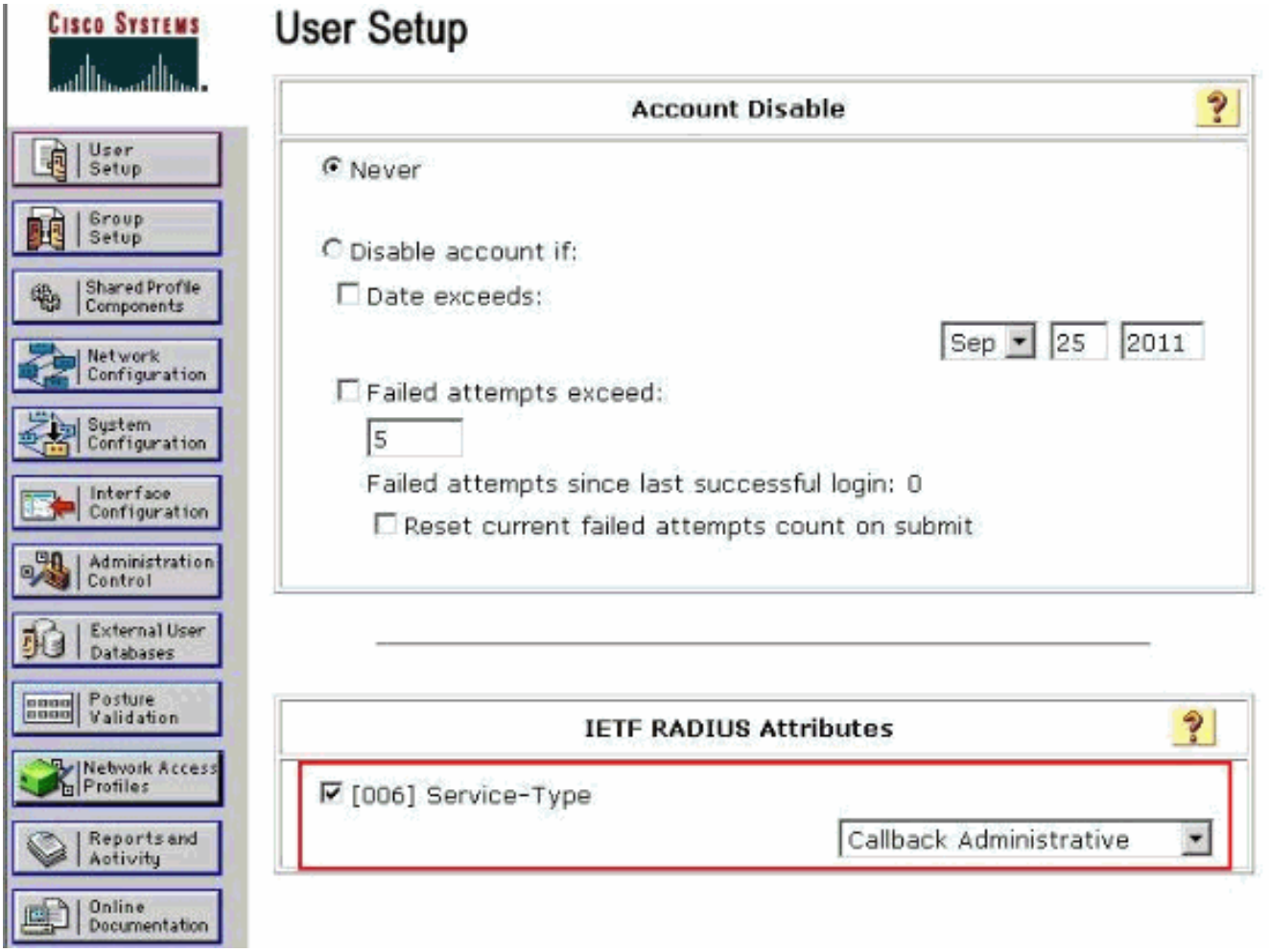
1. 从ACS GUI中，选择User Setup(**用户设置**)选项卡。
2. 输入要添加到ACS的用户名，如以下示例窗口所示：



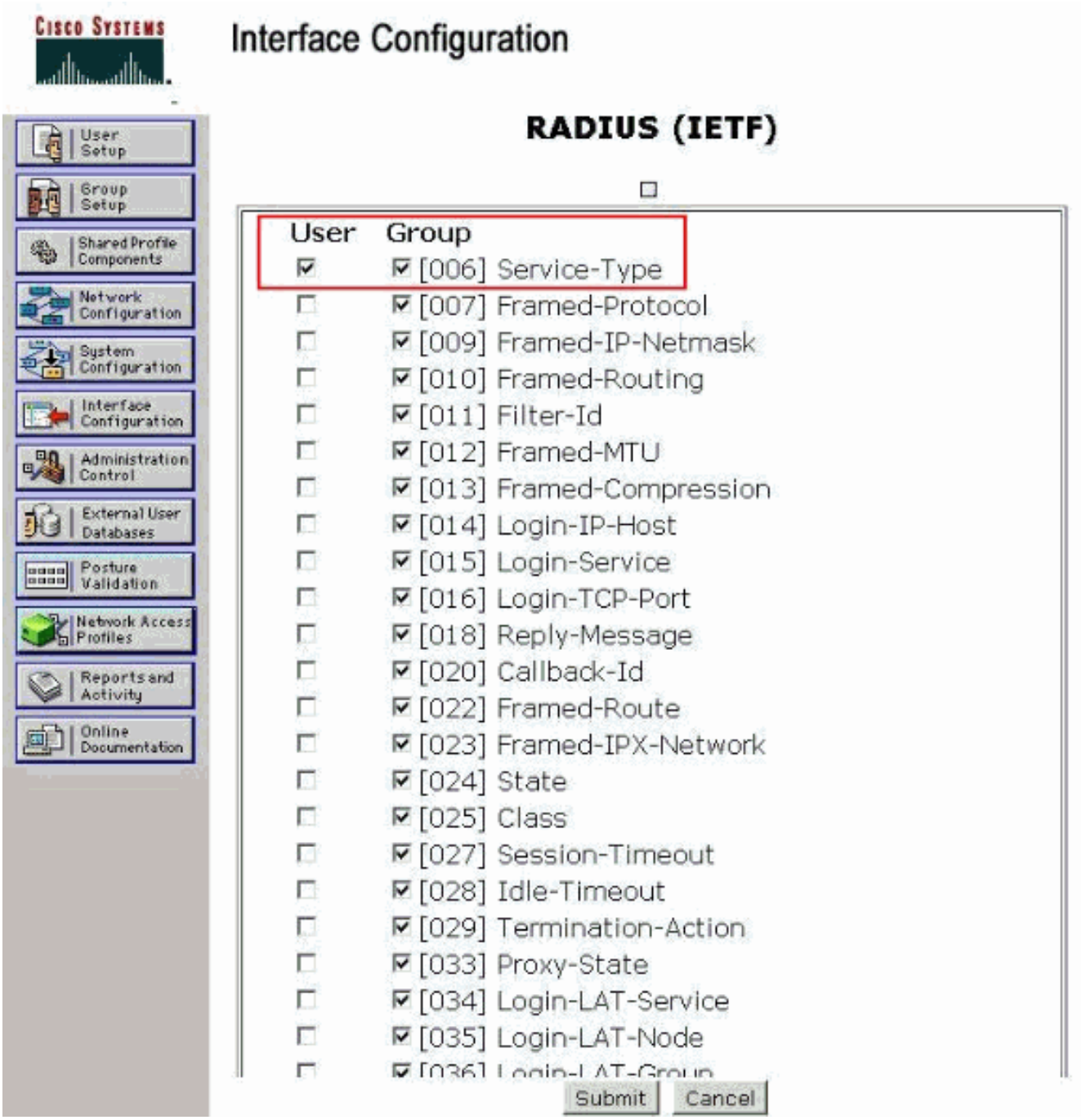
3. 单击**Add/Edit**以转到“User Edit”页。
4. 在“用户编辑”(User Edit)页面上，提供此用户的实名、说明和密码详细信息。在本示例中，使用的用户名和密码均为lobbyadmin。



5. 向下滚动到IETF RADIUS Attributes设置并选中Service-Type Attribute**复选框。**
6. 从“服务类**型”下**拉菜单中选择“回叫管理”，然后单击“**提交”**。这是为此用户分配大厅管理员角色的属性。



有时，此服务类型属性在用户设置下不可见。在这种情况下，请完成以下步骤使其可见：从ACS GUI中，选择**Interface Configuration > RADIUS(IETF)**以在User Configuration窗口中启用IETF属性。这将进入RADIUS(IETF)设置页面。从RADIUS(IETF)Settings页面，您可以启用需要在用户或组设置下可见的IETF属性。对于此配置，请选**中"用户"**列的"服务类型"并单**击提交**。此窗口显示一个示例
：



注意：此示例按用户指定身份验证。您还可以根据特定用户所属的组执行身份验证。在这种情况下，请选中**Group**复选框，以便此属性在Group设置下可见。**注意：**此外，如果身份验证基于组，则需要将用户分配到特定组，并配置组设置IETF属性以向该组的用户提供访问权限。有关如何配置和管理组的详细信息，请参阅用户组管理。

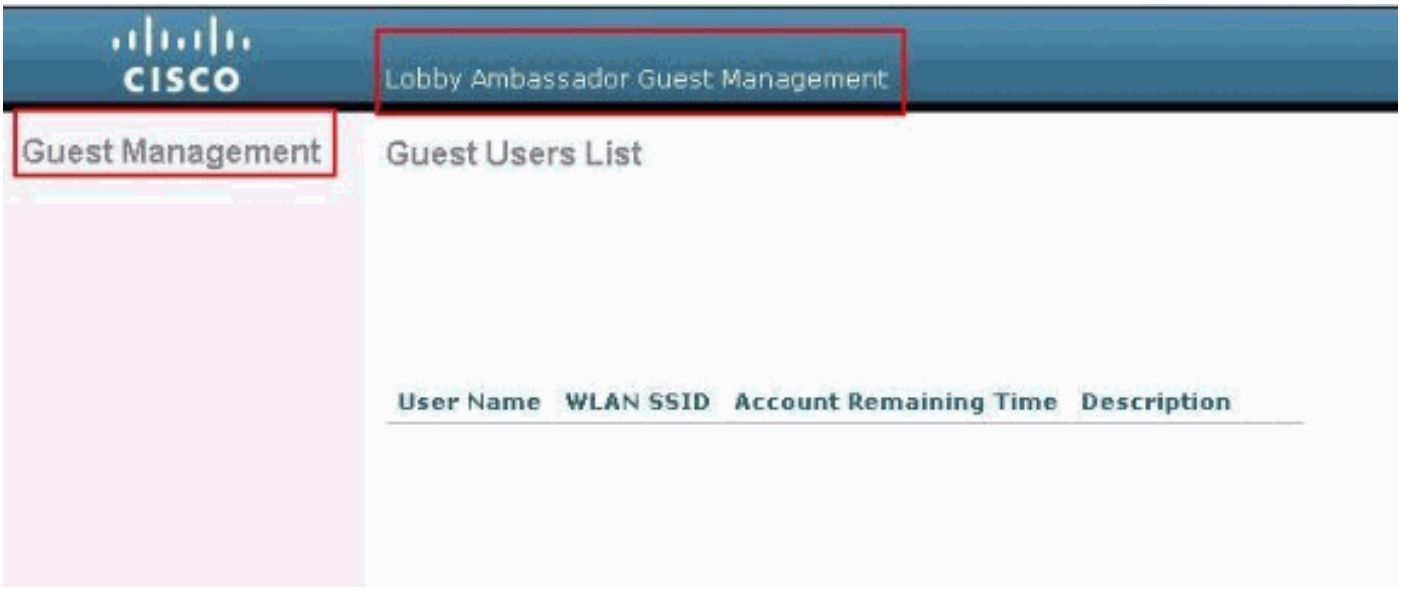
验证

使用本部分可确认配置能否正常运行。

要验证配置是否正常工作，请通过GUI(HTTP/HTTPS)模式访问WLC。

注意：大厅大使无法访问控制器CLI界面，因此只能从控制器GUI创建访客用户帐户。

当出现登录提示时，输入在ACS上配置的用户名和密码。如果配置正确，您将作为大厅管理员成功通过WLC**的身份验证**。此示例显示大厅管理员的GUI如何处理成功的身份验证：



注意：您可以看到，大厅管理员除了访客用户管理之外没有其他选项。

要从CLI模式验证它，请以读写管理员身份Telnet至控制器。在控制器CLI**上发出debug aaa all enable命令。**

```
(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
```

在此输出中突出显示的信息中，您可以看到服务类型属性11（回叫管理）从ACS服务器传递到控制器，并且用户以大厅管理员身份登录。

以下命令可能会提供额外帮助：

- debug aaa details enable
- debug aaa events enable
- debug aaa packets enable

注意：在使用debug命令之前，请参阅有关Debug命令的重要信息。

故障排除

当您登录到具有接待大使权限的控制器时，您无法创建具有“0”生命时间值的访客用户帐户，该帐户永不过期。在这些情况下，您会收到`Lifetime value cannot be 0`误消息。

这是由于Cisco Bug ID CSCsf32392（仅限注册客户）（主要在WLC版本4.0中找到）。此Bug已在WLC版本4.1中解决。

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
- 思科无线 LAN 控制器配置指南，第 4.0 版 - 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