管理用户的RADIUS服务器验证无线局域网控制器(WLC)配置示例的

目录

简介

本文解释如何配置无线局域网控制器(WLC)和访问控制服务器(Cisco Secure ACS)，以便AAA服务器能验证控制器的管理用户。本文也解释不同的管理用户如何能接收不同的权限使用从Cisco Secure ACS RADIUS服务器(VSAs)返回的供应商专用属性。

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服务器类似Cisco Secure ACS

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 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

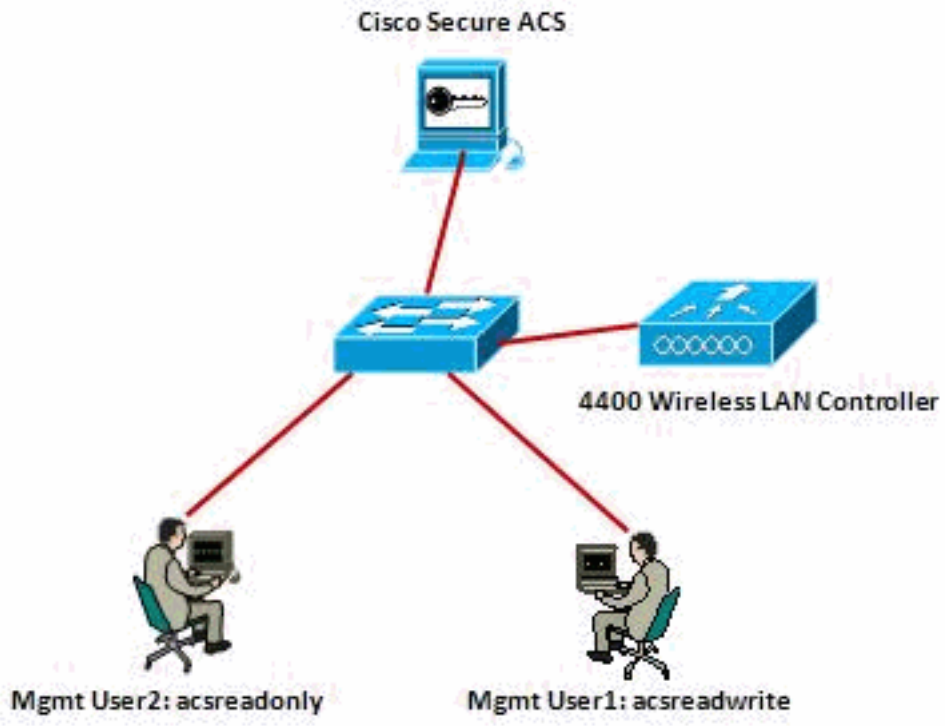
有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

在此部分，您提交与关于如何的信息配置WLC和ACS在本文描述的目的。

网络图

本文档使用以下网络设置：



此配置示例使用这些参数：

- Cisco Secure ACS的IP地址— 172.16.1.1/255.255.0.0
- 控制器的管理接口IP地址— 172.16.1.30/255.255.0.0
- 在接入点(AP)和RADIUS服务器使用— asdf1234的共享密钥
- 这些是此示例在ACS配置两个用户的凭证：用户名- acsreadwrite密码- acsreadwrite用户名- acsreadonly密码- acsreadonly

您需要配置WLC和Cisco Secure Cisco Secure ACS为了：

- 登录与用户名和密码的WLC的任何用户，当**acsreadwrite**给对WLC的全双工管理访问。
- 登录与用户名和密码的WLC的任何用户，当**acsreadonly**给对WLC的只读访问。

配置

本文档使用以下配置：

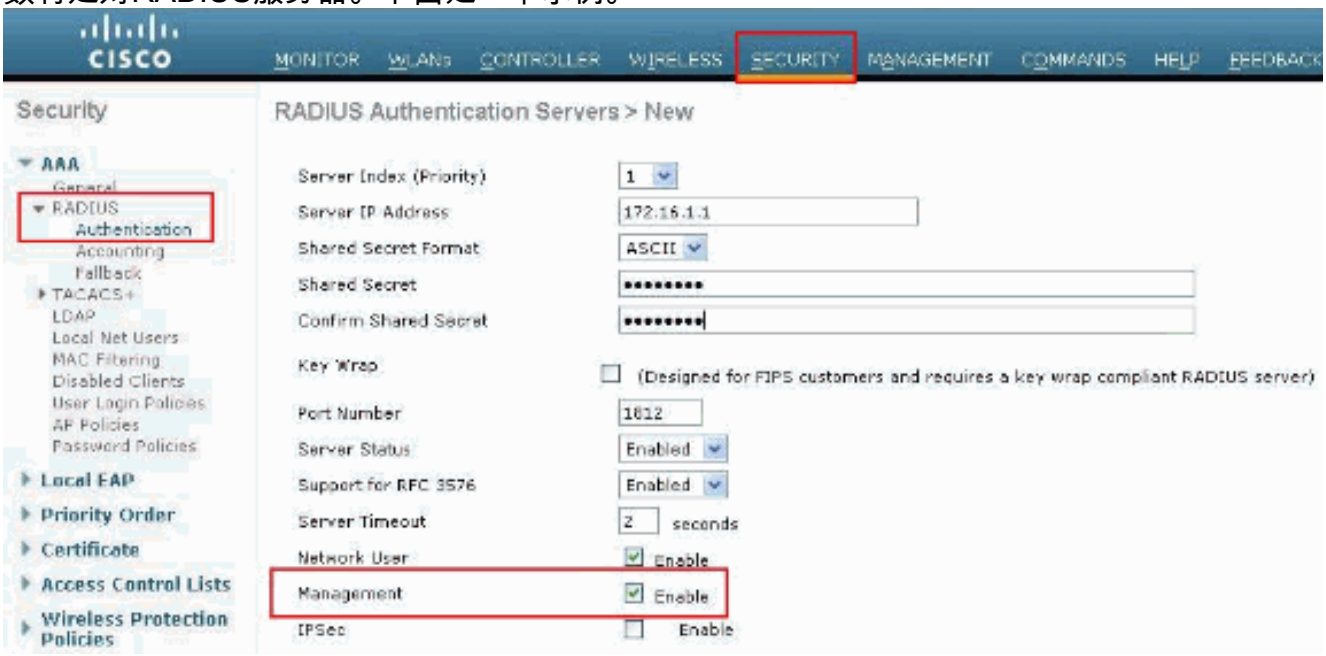
- WLC 配置
- Cisco Secure ACS配置

WLC 配置

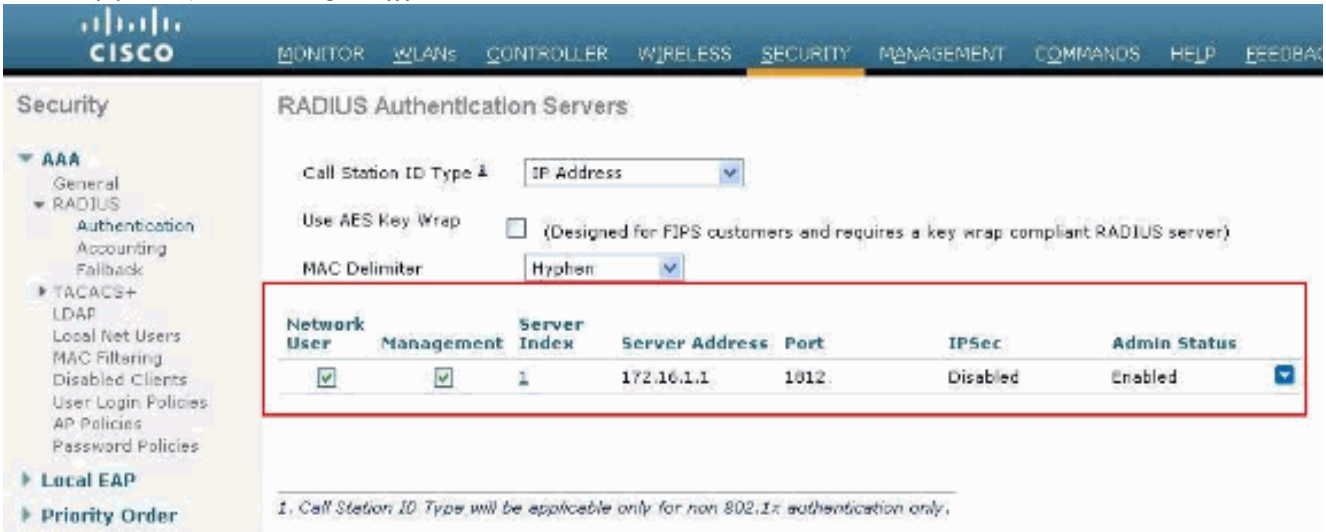
配置WLC通过Cisco Secure ACS服务器接受管理

完成这些步骤为了配置WLC，以便能与RADIUS服务器联络。

1. 从 WLC GUI 中，单击 **Security**。从在左边的菜单，请点击**RADIUS>验证。RADIUS验证服务器**页出版。添加一个新的RADIUS服务器，点击**新**。在**RADIUS验证服务器>New**页，请输入参数特定对RADIUS服务器。下面是一个示例。



2. 检查**管理**单选按钮为了允许RADIUS服务器验证登陆对WLC的用户。**注意：** 保证在此页配置的共享机密配比与在RADIUS服务器配置的共享机密。WLC能与RADIUS服务器那时联络。
3. 验证WLC是否配置由Cisco Secure ACS管理。为了执行此，请点击从WLC GUI的**安全**。产生的GUI窗口看起来与此示例相似。



您能看到**管理**复选框为RADIUS服务器172.16.1.1启用。这说明ACS允许验证WLC的管理用户。

Cisco Secure ACS配置

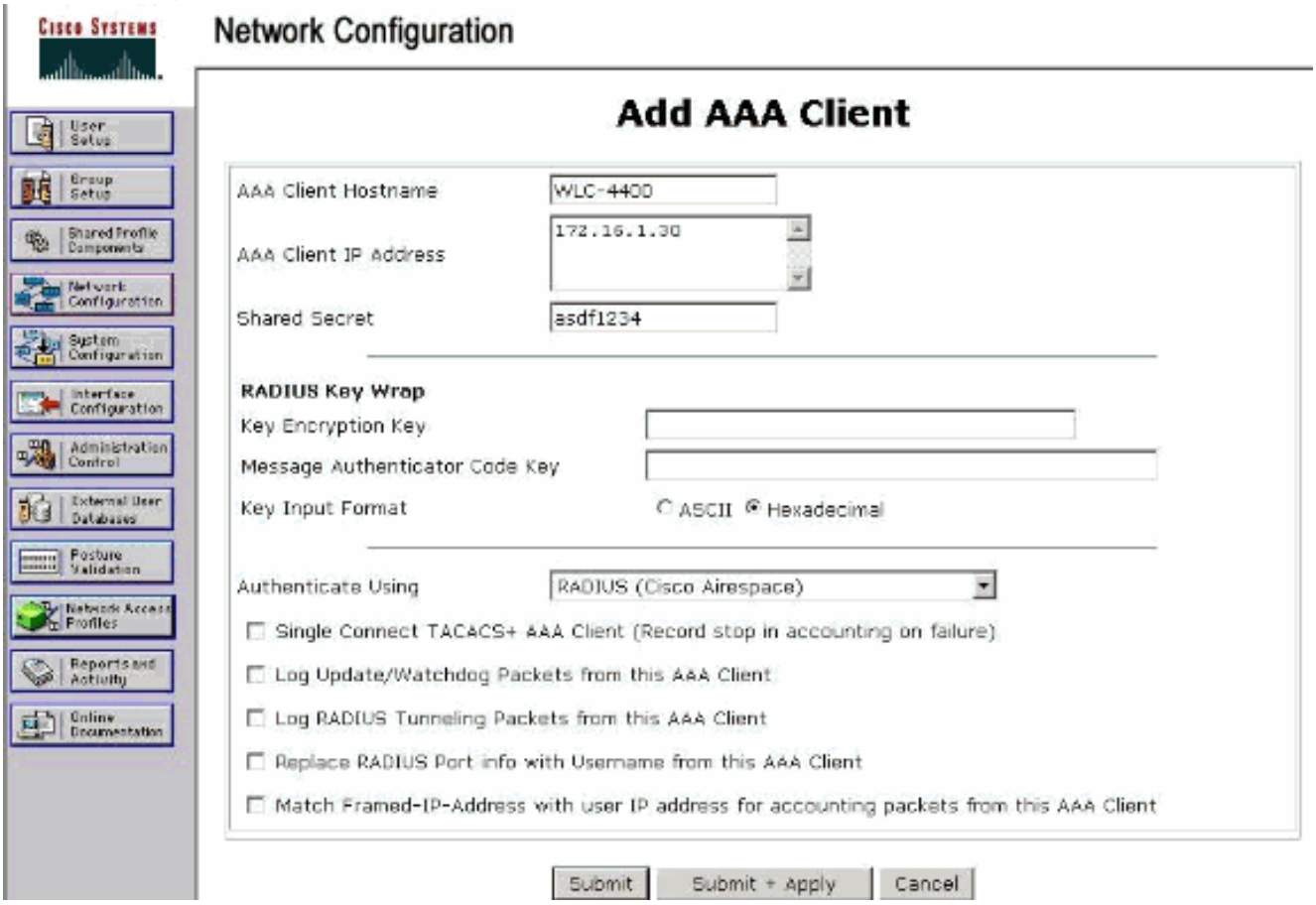
完成在这些部分的步骤为了配置ACS ：

1. 添加WLC作为AAA客户端到RADIUS服务器。
2. 配置用户和他们适当的RADIUS IETF属性。
3. 配置有读写访问的一个用户。
4. 配置有只读访问的一个用户。

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Cisco Secure ACS的一个AAA客户端。

1. 从 ACS GUI 中，单击 **Network Configuration**。
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。在本例中，这些是设置：AAA客户端主机名是WLC-4400172.16.1.30/16是AAA客户端IP地址，在这种情况下是WLC。共享密钥是"asdf1234"。



这共享的密钥必须是相同的象您在WLC配置的共享密钥。

4. 从验证使用下拉菜单，请选择**RADIUS (思科Airespace)**。
5. 点击**Submit+Restart**为了保存配置。

配置用户和他们适当的RADIUS IETF属性

为了通过一个RADIUS服务器验证用户，控制器登录和管理的，您必须添加用户到RADIUS数据库IETF RADIUS属性*服务类型*设置对appropriate值根据用户的权限。

- 为了设置用户的读写权限，设置类型属性对**管理**。
- 为了设置用户的只读权限，设置类型属性为**Nas提示**。

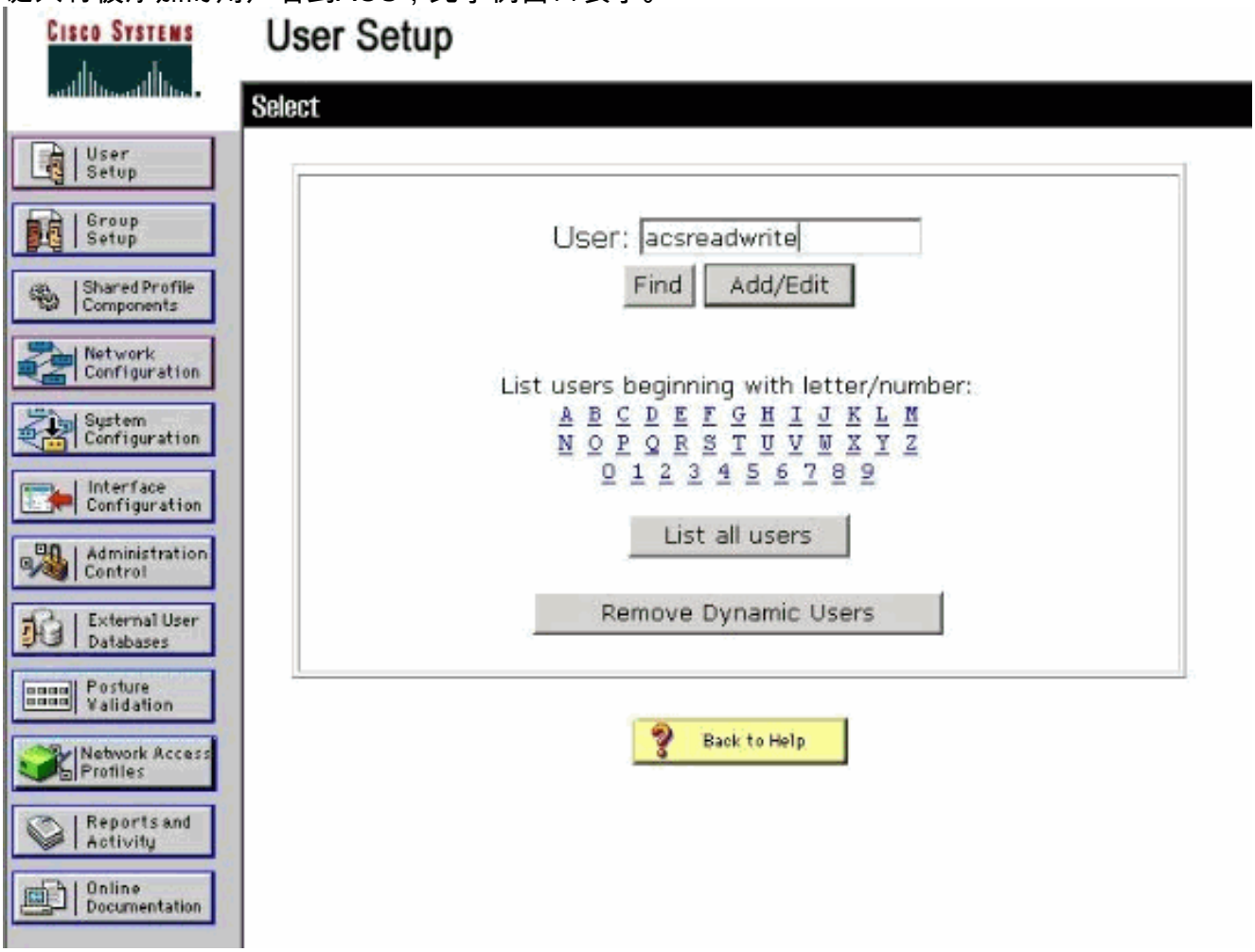
配置有读写访问的用户

第一示例显示一个用户的配置有完全权限的对WLC。当此用户设法登录到控制器时， RADIUS服务器验证并且提供此用户全双工管理访问。

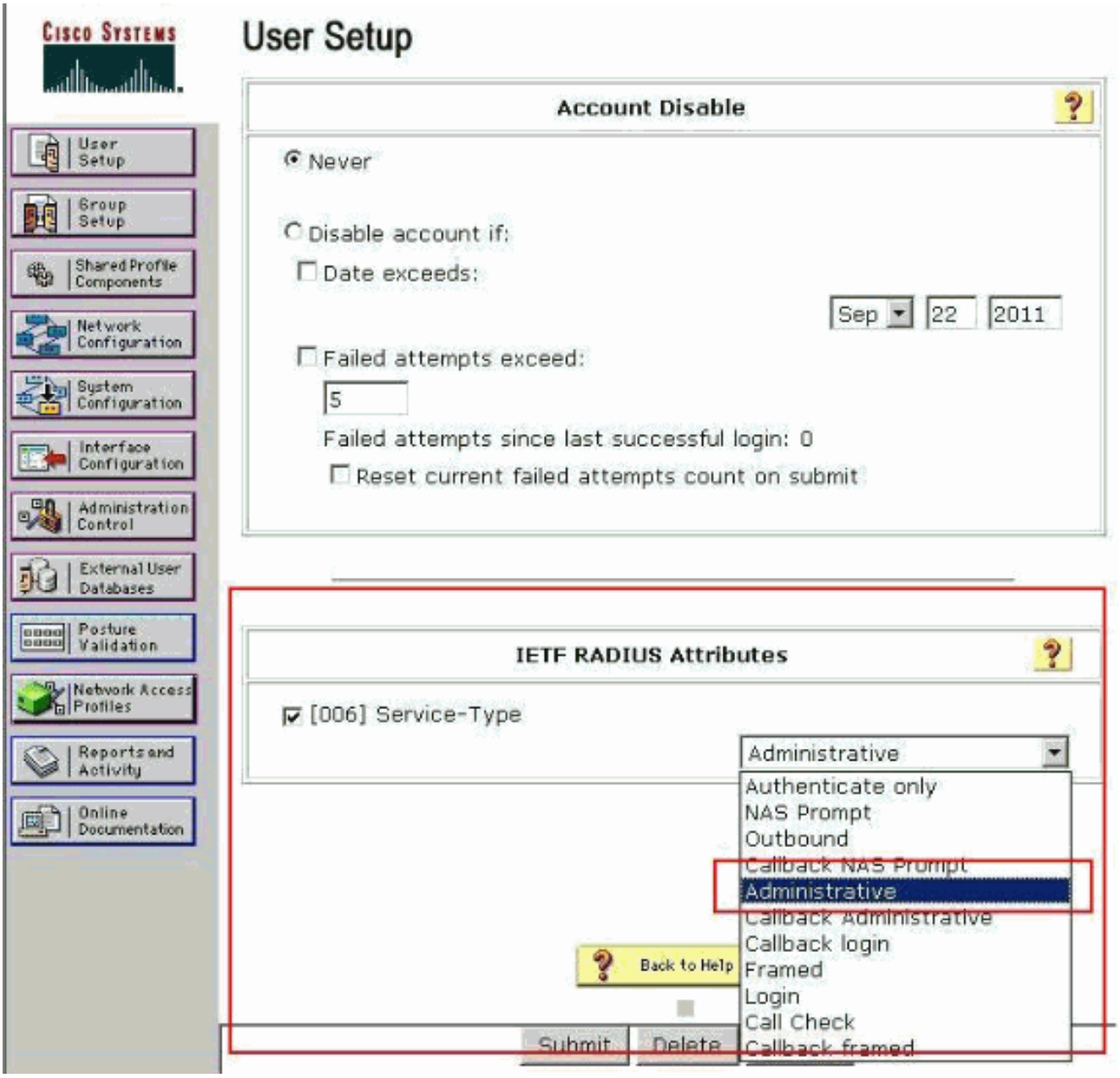
在本例中，用户名和密码是**acsreadwrite**。

完成在Cisco Secure ACS的这些步骤。

1. 从 ACS GUI 中，单击 **User Setup**。
2. 键入将被添加的用户名到ACS，此示例窗口表示。

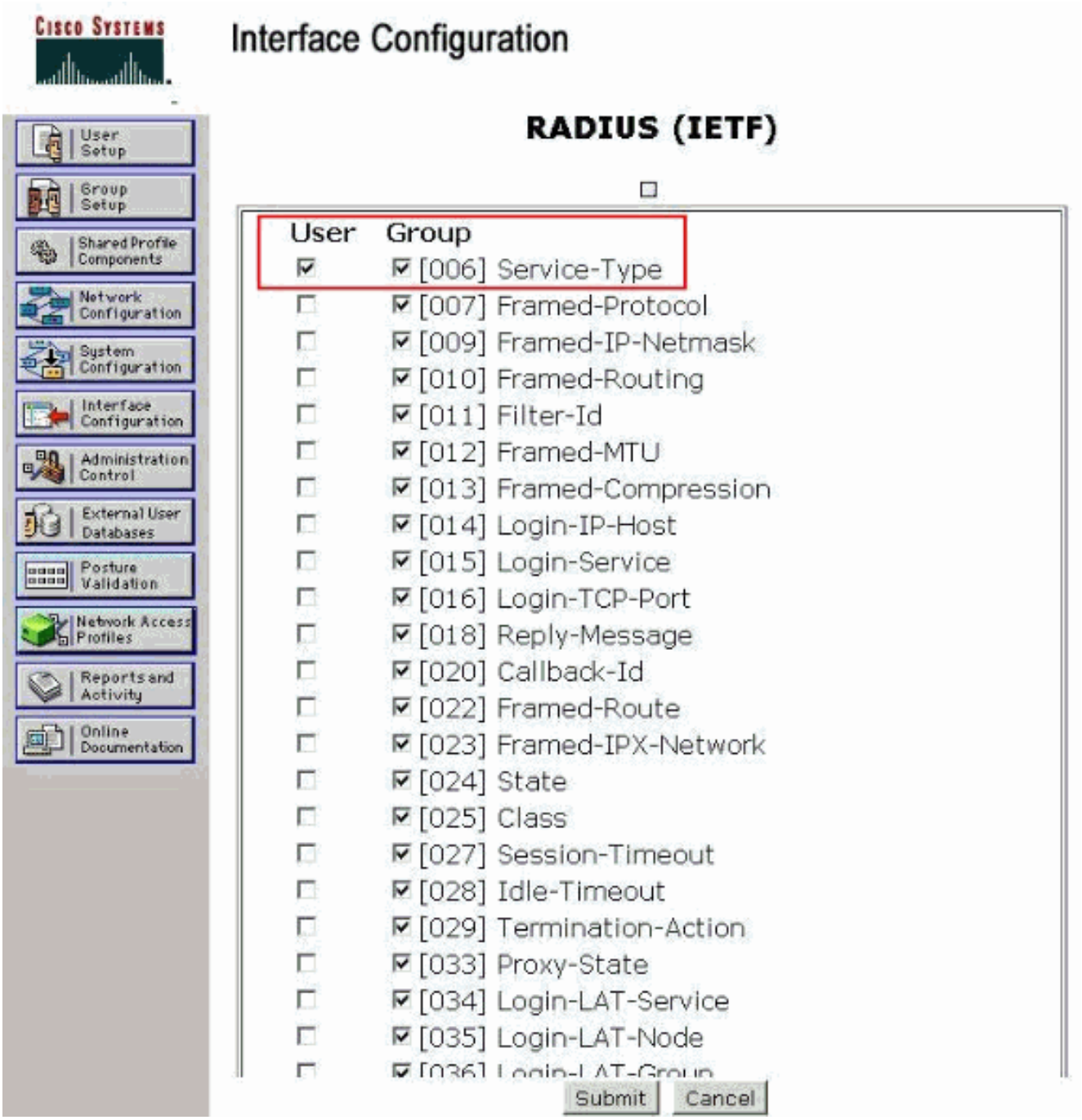


3. 单击**添加/编辑**为了去Edit页的用户。
4. 在Edit页的用户，请提供此用户真名、说明和密码细节。
5. 移下来对设置IETF的RADIUS属性并且检查**类型属性**。
6. 因为，在本例中，用户acsreadwrite需要给完全权限，请选择**管理**服务类型下拉菜单的并且单击**提交**。这保证此特定用户访问读写访问WLC。



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。

1. 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。这把您带对Settings页的RADIUS (IETF)。
2. 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，请启用**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。关于如何的参考的组管理配置与管理组的详细信息。

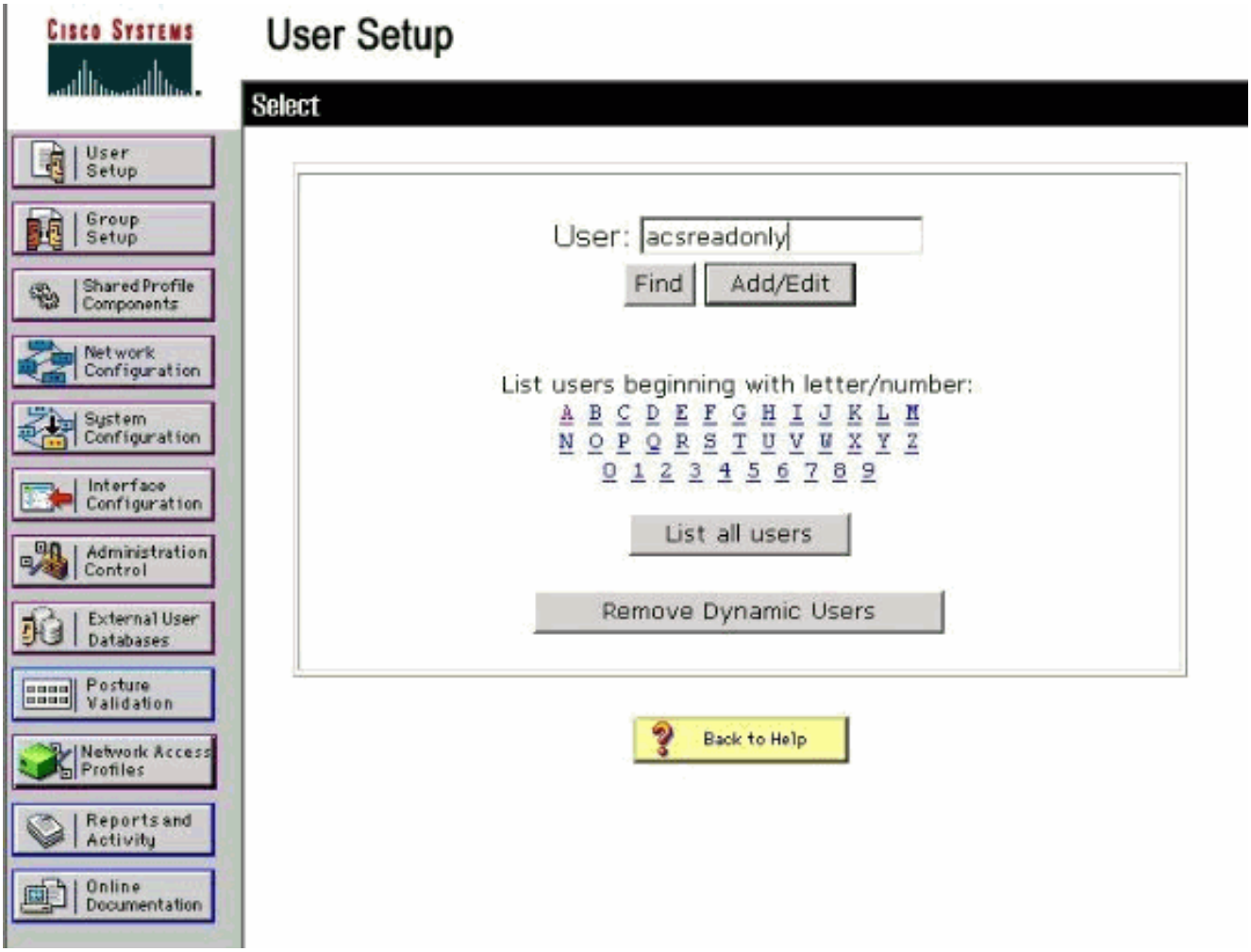
配置有只读访问的用户

此示例显示一个用户的配置有只读访问的对WLC。当此用户设法登录到控制器时， RADIUS服务器验证并且提供此用户只读访问。

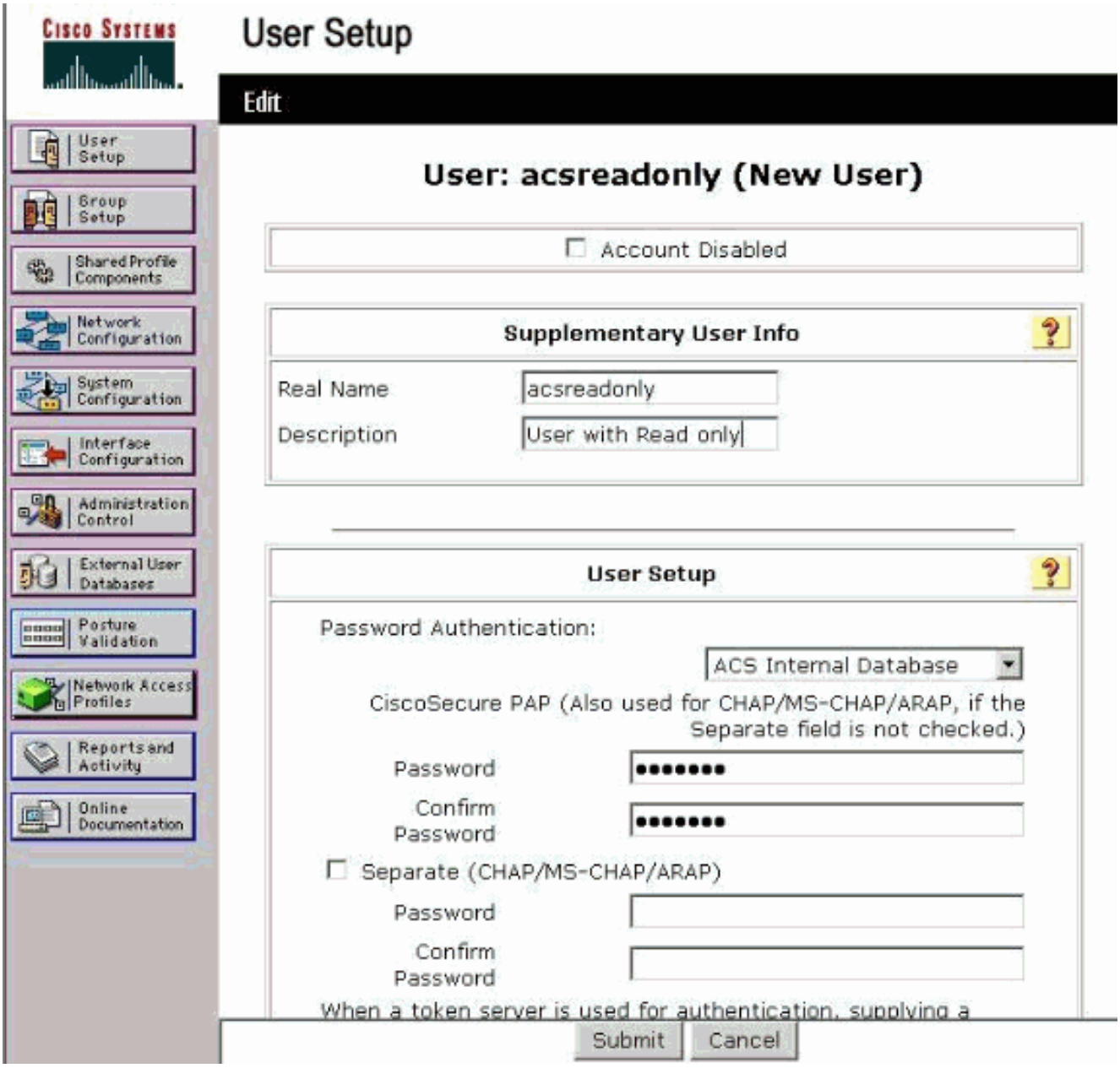
在本例中，用户名和密码是**acsreadonly**。

在 Cisco Secure ACS 上完成以下步骤：

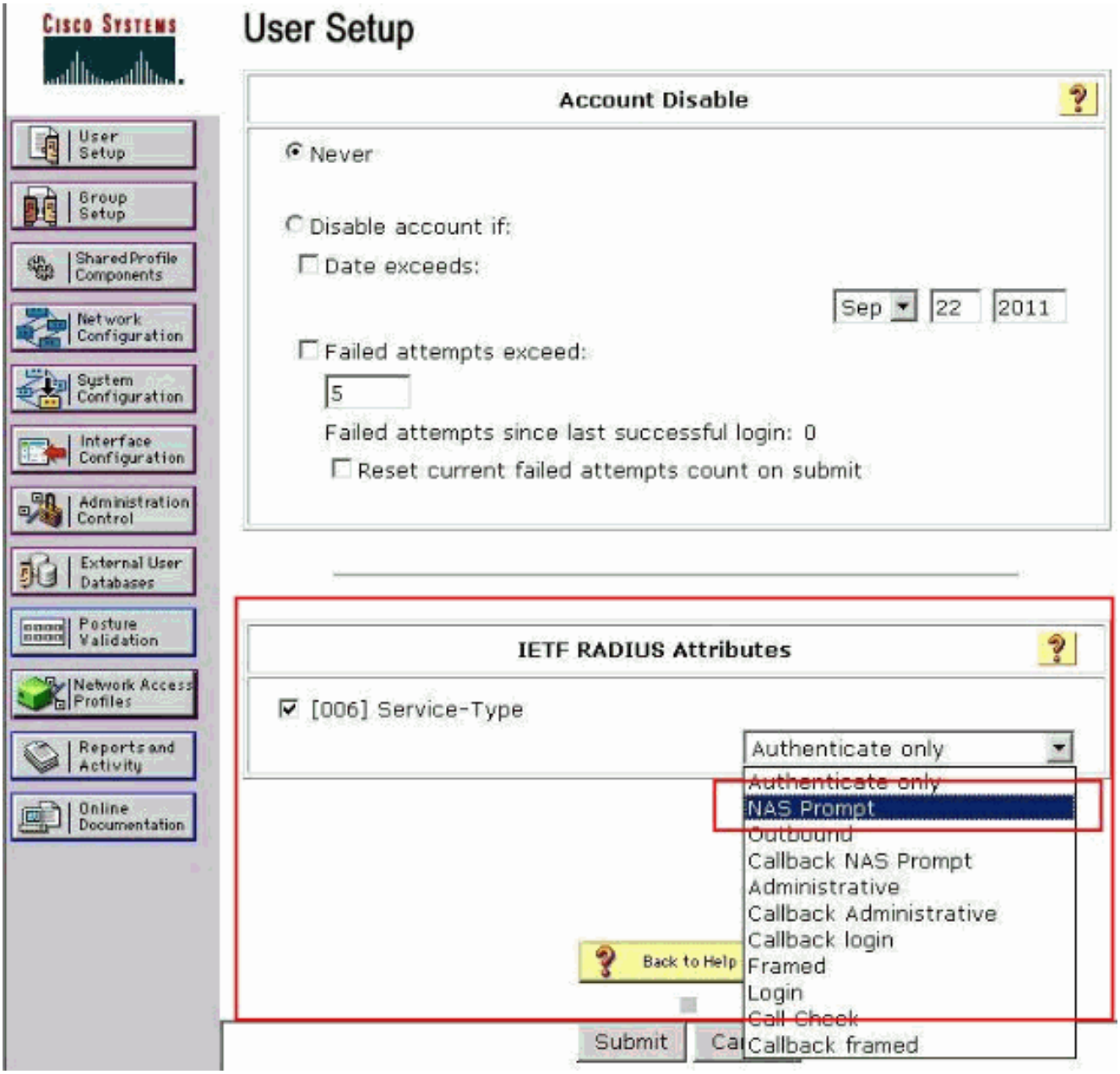
1. 从 ACS GUI 中，单击 **User Setup**。
2. 键入您想要添加对ACS的用户名并且单击**添加/编辑**为了去Edit页的用户。



3. 提供此用户真名、说明和密码。此窗口表示示例。

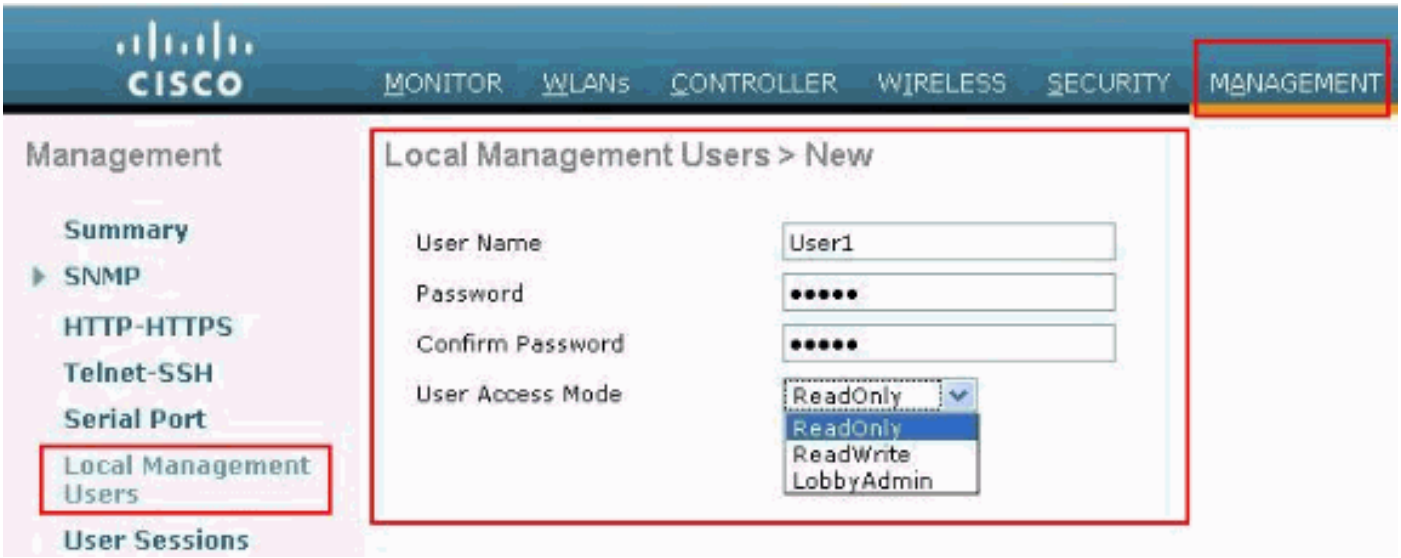


4. 移下来对设置IETF的RADIUS属性并且检查**类型属性**。
5. 因为，在本例中，用户acsreadonly需要访问只读访问，选择**NAS**从服务类型下拉菜单**提示**并且单击**提交**。这保证此特定用户访问只读访问WLC。



[管理WLC本地以及通过RADIUS服务器]

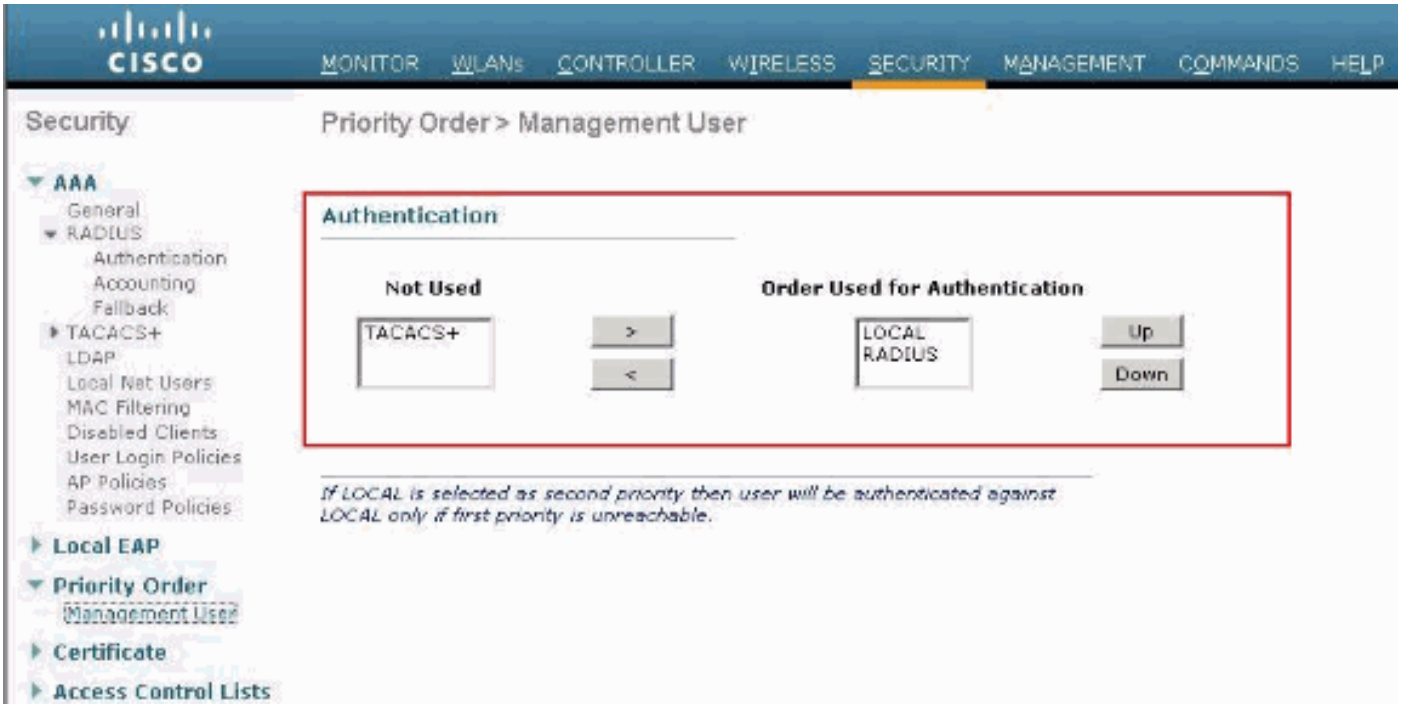
您在WLC能本地也配置管理用户。这可以从控制器GUI执行，在**Management>本地管理用户下。**



假设， WLC配置与管理用户本地以及在RADIUS服务器用启用的**管理**复选框。在这种情况下，默认情况下，当用户设法登录到WLC时， WLC如此正常运行：

1. WLC首先查看本地管理用户定义验证用户。如果用户在其当地资料目录存在，则允许验证此用户。如果此用户没出现本地，则它查找到RADIUS服务器。
2. 如果同一个用户存在本地以及在RADIUS服务器，但是用不同的访问权限，则WLC验证用户有指定的权限本地。换句话说，在WLC的本地配置总是获得优先权，当与RADIUS服务器比较。

验证命令管理用户的在WLC可以更改。为了执行此，从在WLC的**安全页**，点击**优先级命令>管理用户**。从此页您能指定验证命令。下面是一个示例。



注意： 如果本地其次选择作为优先级，则用户将验证使用此方法，只有当作为最优先考虑的事定义的方法(RADIUS/TACACS)是不可得到的。

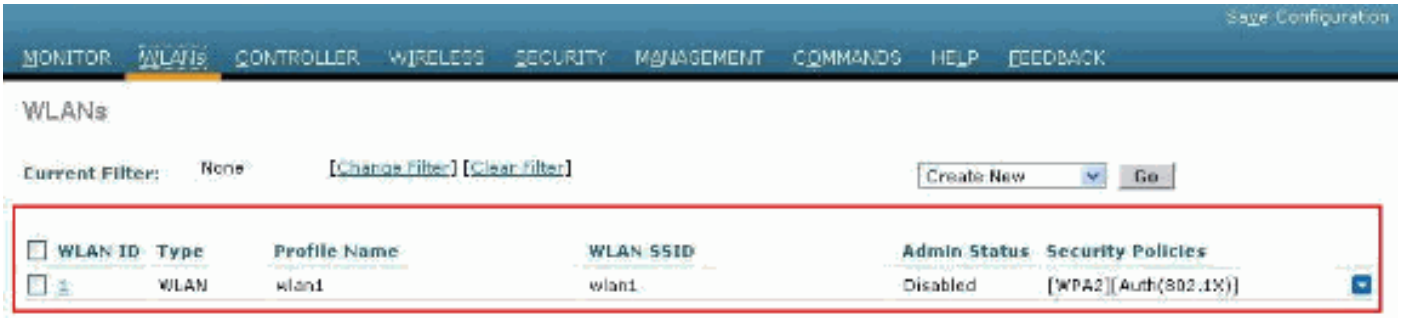
验证

为了验证适当您的配置工作，是否通过CLI或GUI (HTTP/HTTPS)模式访问WLC。当登录提示出现时，请键入用户名和密码如配置在Cisco Secure ACS。

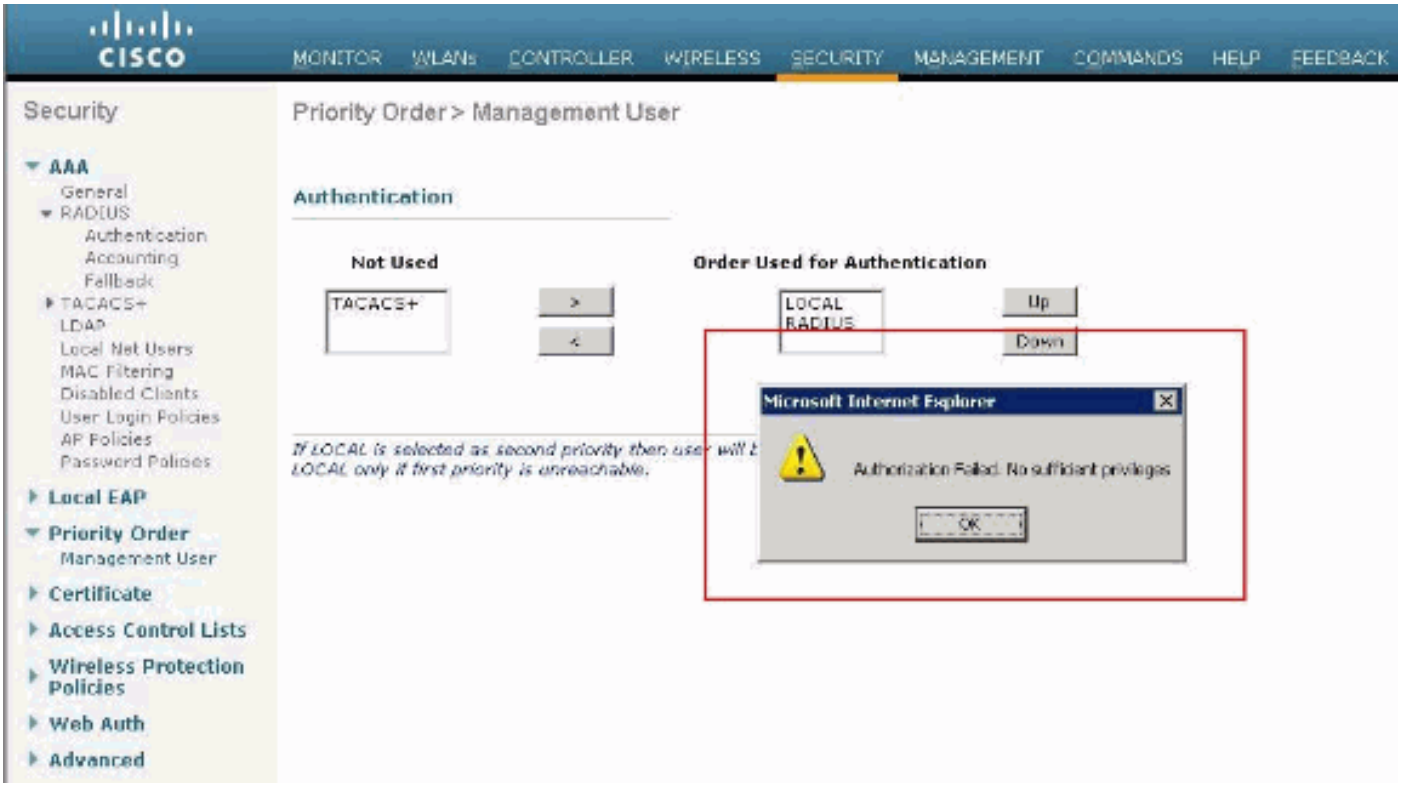
如果有正确的配置，您顺利地验证到WLC。

您能也保证已认证的用户是否带有访问限制如指定由ACS。为了执行如此，请通过HTTP/HTTPS访问WLC GUI (请保证WLC配置允许HTTP/HTTPS)。

一个用户在ACS设置的读写访问有几种可配置权限在WLC。例如，一个读写用户有权限创建一新的WLAN在WLC的WLAN页下。此窗口表示示例。



当有只读provileges的一个用户设法修改在控制器时的配置，用户看到此消息。



这些访问限制可能通过WLC的CLI也验证。下面是一个输出示例。

```
(Cisco Controller) >? debug Manages system debug options. help Help linktest Perform a link test
to a specified MAC address. logout Exit this session. Any unsaved changes are lost. show Display
switch options and settings. (Cisco Controller) >config Incorrect usage. Use the '?' or <TAB>
key to list commands.
```

此示例输出显示， a **?** 在控制器CLI显示可以使用的命令列表当前用户的。并且请注意**config命令不**是可用的在此示例输出中。这说明一个只读用户没有权限执行在WLC的任何配置。而，一个读写用户有权限对在控制器的DID配置(GUI和CLI模式)。

注意： 在您通过RADIUS服务器以后验证WLC用户，因为您从页浏览到页， HTTP [S]服务器每次充分地仍然验证客户端。没有提示对于在每个页的验证的唯一的原因是您的浏览器缓存并且重赛您的凭证。

故障排除

有某些情况，当控制器通过ACS成功验证管理用户，验证完成(access-accept)时，并且您看不到在控制器的所有授权错误。*但是，再提示用户输入验证。*

在这类情况下，您不能解释什么是错误，并且用户为什么不能登录WLC由使用**enable命令debug**

aaa的事件。反而，控制器显示另一提示输入验证。

此的一个可能的来源是ACS没有配置传送该特定用户或组的类型属性，即使用户名和密码在ACS正确地配置。

enable命令debug aaa的事件的输出不表明用户没有需要的属性(此示例，类型属性)，即使**access-accept**从AAA服务器是被退还的。此示例**debug aaa事件enable命令**输出显示示例。

```
 (Cisco Controller) >debug aaa events enable Mon Aug 13 20:14:33 2011: AuthenticationRequest:
0xa449a8c Mon Aug 13 20:14:33 2011: Callback.....................................0x8250c40 Mon
Aug 13 20:14:33 2011: protocolType.................................0x00020001 Mon Aug 13
20:14:33 2011: proxyState.....................1A:00:00:00:00:00-00:00 Mon Aug 13 20:14:33 2011:
Packet contains 5 AVPs (not shown) Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Successful
transmission of Authentication Packet (id 8) to 172.16.1.1:1812, proxy state 1a:00:00:00:00:00-
00:00 Mon Aug 13 20:14:33 2011: ****Enter processIncomingMessages: response code=2 Mon Aug 13
20:14:33 2011: ****Enter processRadiusResponse: response code=2 Mon Aug 13 20:14:33 2011:
1a:00:00:00:00:00 Access-Accept received from RADIUS server 172.16.1.1 for mobile
1a:00:00:00:00:00 receiveId = 0 Mon Aug 13 20:14:33 2011: AuthorizationResponse: 0x9802520 Mon
Aug 13 20:14:33 2011: structureSize.............................28 Mon Aug 13 20:14:33 2011:
resultCode.....................................0 Mon Aug 13 20:14:33 2011:
protocolUsed.................................0x00000001 Mon Aug 13 20:14:33 2011:
proxyState.....................1A:00:00:00:00:00-00:00 Mon Aug 13 20:14:33 2011: Packet
contains 0 AVPs:
```

在此第一个示例**debug aaa事件enable命令**输出，您看到Access-Accept从RADIUS服务器顺利地接收，但是类型属性没有通过在WLC上。这是因为特定用户没有配置与在ACS的此属性。

Cisco Secure ACS需要配置在用户认证以后返回类型属性。必须设置服务类型属性值为**管理**或**Nas提示**根据用户权限。

此第二示例再显示**debug aaa事件enable命令**输出。然而，这次类型属性设置对**管理**在ACS。

```
(Cisco Controller)>debug aaa events enable Mon Aug 13 20:17:02 2011: AuthenticationRequest:
0xa449f1c Mon Aug 13 20:17:02 2011: Callback.....................................0x8250c40 Mon
Aug 13 20:17:02 2011: protocolType.................................0x00020001 Mon Aug 13
20:17:02 2011: proxyState.....................1D:00:00:00:00:00-00:00 Mon Aug 13 20:17:02
2011: Packet contains 5 AVPs (not shown) Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Successful
transmission of Authentication Packet (id 11) to 172.16.1.1:1812, proxy state 1d:00:00:00:00:00-
00:00 Mon Aug 13 20:17:02 2011: ****Enter processIncomingMessages: response code=2 Mon Aug 13
20:17:02 2011: ****Enter processRadiusResponse: response code=2 Mon Aug 13 20:17:02 2011:
1d:00:00:00:00:00 Access-Accept received from RADIUS server 172.16.1.1 for mobile
1d:00:00:00:00:00 receiveId = 0 Mon Aug 13 20:17:02 2011: AuthorizationResponse: 0x9802520 Mon
Aug 13 20:17:02 2011: structureSize.............................100 Mon Aug 13 20:17:02 2011:
resultCode.....................................0 Mon Aug 13 20:17:02 2011:
protocolUsed.................................0x00000001 Mon Aug 13 20:17:02 2011:
proxyState.....................1D:00:00:00:00:00-00:00 Mon Aug 13 20:17:02 2011: Packet
contains 2 AVPs: Mon Aug 13 20:17:02 2011: AVP[01] Service-Type...........0x00000006 (6) (4
bytes) Mon Aug 13 20:17:02 2011: AVP[02] Class......... CISCOACS:000d1b9f/ac100128/acsserver (36
bytes)
```

您在此示例输出中能看到类型属性通过在WLC上。

相关信息

- 配置无线局域网控制器配置指南
- 无线局域网控制器上的 VLAN 配置示例
- 带有RADIUS服务器的动态VLAN分配和无线局域网控制器的配置示例
- 无线 LAN 控制器和轻量接入点基本配置示例

- 具有无线局域网控制器的 AP 组 VLAN 配置示例
- 技术支持和文档 - Cisco Systems