

# 无线局域网无线控制器管理用户 通过 RADIUS 服务器认证的配置举例

简介 .....	2
先决条件 .....	2
要求 .....	2
组件使用 .....	2
配置 .....	2
网络图 .....	2
无线控制器的配置 .....	3
思科 SECURE ACS 的配置 .....	4
将无线控制器作为 AAA 客户端添加到 RADIUS 服务器 .....	5
配置用户和其相应的 RADIUS IETF 属性。 .....	6
配置具有读写访问权限的用户 .....	6
配置只读访问用户 .....	8
无线控制器本地管理用户 .....	11
验证 .....	12
故障排查 .....	14

# 简介

本文档介绍了如何配置无线控制器（WLC）和访问控制服务器（思科 Secure ACS 的），使得 AAA 服务器可以对无线控制器进行管理用户的身份验证。还介绍了如何使用从思科 Secure ACS 的 RADIUS 服务器返回的供应商特定属性(VSA)使不同的管理用户可以得到不同的权限。

## 先决条件

### 要求

确保满足下列要求再尝试配置：

- \*了解如何在无线控制器上配置基本参数
- \*了解如何配置 RADIUS 服务器，例如思科 Secure ACS 的知识

### 组件使用

本文档中的信息基于下列软件和硬件版本：

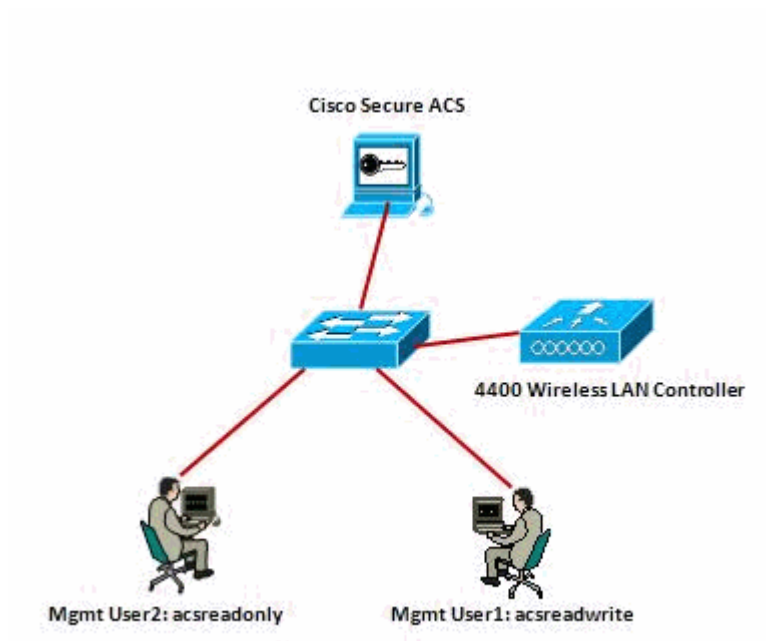
- \*运行 7.0.216.0 版本的思科 4400 无线控制器
- \*配置为 RADIUS 服务器的思科 Secure ACS，使用软件版本 4.1。

本文档中的资料是从一个特定实验室环境中的设备上生成的。本文档中使用的所有设备以缺省（默认）配置开始配置。如果您的网络是正在使用的生产系统，请确保您了解所有命令带来的潜在影响。

## 配置

### 网络图

本文使用的网络设置如下图所示：



此配置示例使用下列参数：

- \*思科 Secure ACS 的 IP 地址 - 172.16.1.1/255.255.0.0
- \*无线控制器管理接口的 IP 地址 - 172.16.1.30/255.255.0.0
- \*无线控制器和 RADIUS 服务器使用的共享密钥 - asdf1234
- \*在 ACS 配置两个用户的身份凭据：
  - o 用户名 - acsreadwrite；密码 - acsreadwrite
  - o 用户名 - acsreadonly；密码 - acsreadonly

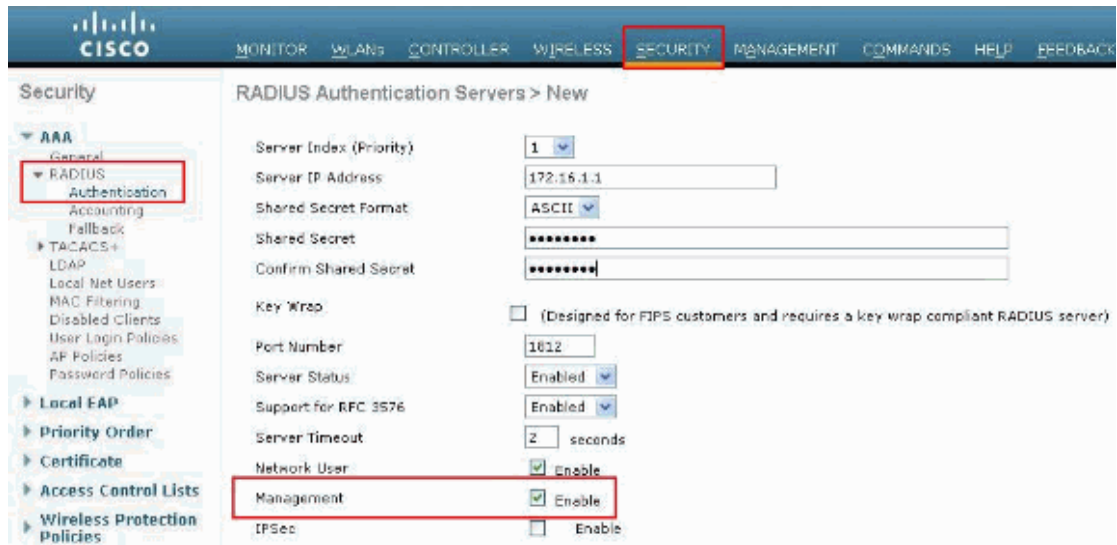
你需要配置无线控制器和思科 Secure ACS 达到下面目的：

- \*任何用户登录到无线控制器的用户名和密码是 acsreadwrite 时，给予其充分的无线控制器的管理访问权限。
- \*任何用户登录到无线控制器的用户名和密码为 acsreadonly 时，无线控制器只能只读访问。

## 无线控制器的配置

配置无线控制器接受在思科 Secure ACS 服务器认证管理用户。完成下列步骤以配置无线控制器，以便它可以与 RADIUS 服务器通信。

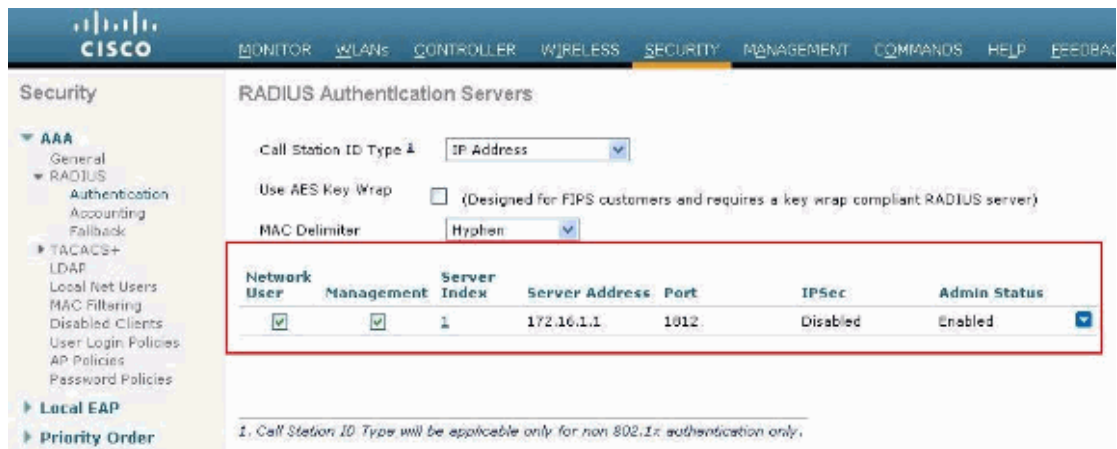
- 1.从无线控制器 GUI 界面单击“安全”。从左侧的菜单中单击 RADIUS > Authentication。RADIUS 认证服务器页面出现。单击新建添加一个新的 RADIUS 服务器。在 RADIUS Authentication Servers > New 页面，输入 RADIUS 服务器的具体参数。下面是一个例子。



2.选择 Management 单选按钮以便让 RADIUS 服务器来验证登录到无线控制器的用户。

注意：请确保此页上配置的共享密钥与 RADIUS 服务器上配置的共享密钥匹配。

3.验证是否在无线控制器上配置了思科 Secure ACS。为了做到这一点，单击安全选项卡。由此产生的 GUI 窗口类似此范例。



你可以看到，RADIUS 服务器 172.16.1.1 启用了 Management 复选框。这说明该 ACS 服务器允许验证无线控制器的管理用户。

## 思科 Secure ACS 的配置

完成下列章节中的步骤，以便配置 ACS：

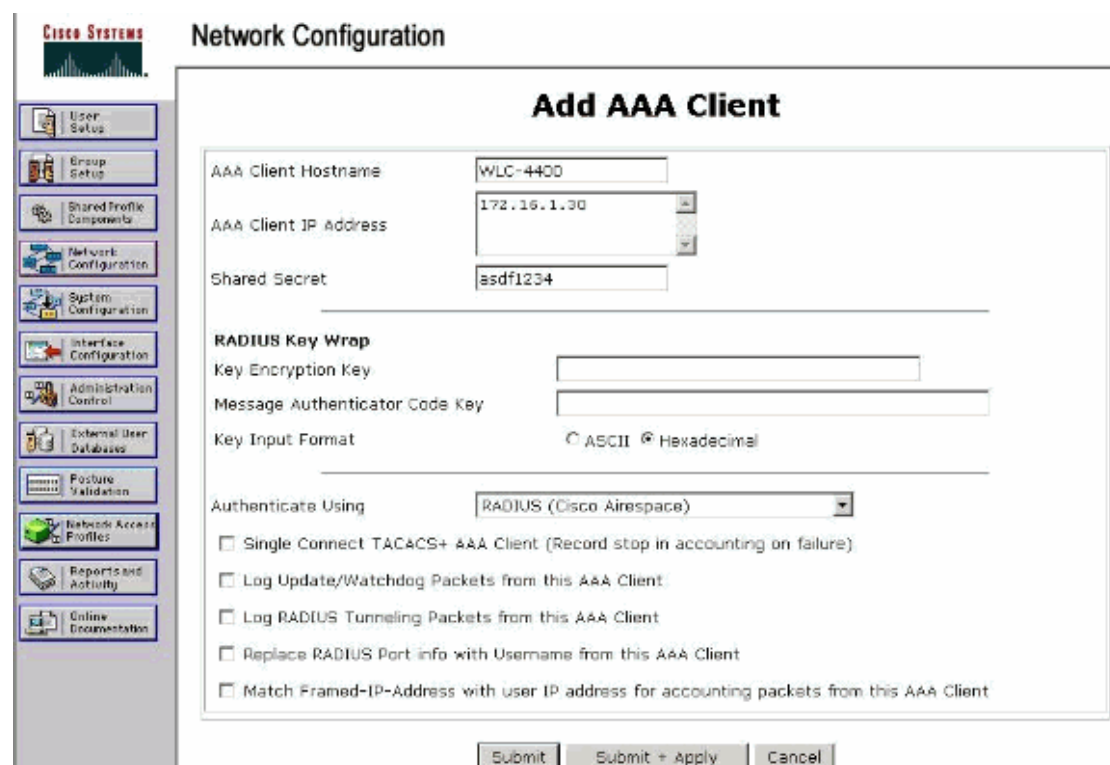
1. 将无线控制器作为 AAA 客户端添加到 RADIUS 服务器
2. 配置用户和其相应的 RADIUS IETF 属性。

3. 配置读写权限的用户。
4. 配置只读访问的用户。

## 将无线控制器作为 AAA 客户端添加到 RADIUS 服务器

在思科 Secure ACS 上完成下列步骤以便增加无线控制器作为 AAA 客户端。

1. 从 ACS 的 GUI 界面单击网络配置 。
2. 在 AAA 客户端处单击添加条目 。
3. 在添加 AAA 客户端的窗口，输入无线控制器的主机名，无线控制器的 IP 地址和共享密钥。  
在这个例子中，这些设置为：
  - \*AAA 客户端的主机名是 WLC-4400
  - \*AAA 客户端的 IP 地址是 172.16.1.30/16。
  - \*共享密钥是 “asdf1234”。



The screenshot shows the 'Add AAA Client' dialog box in the Cisco Secure ACS Network Configuration GUI. The dialog box is titled 'Add AAA Client' and contains the following fields and options:

- AAA Client Hostname: WLC-4400
- AAA Client IP Address: 172.16.1.30
- Shared Secret: asdf1234
- RADIUS Key Wrap**
  - Key Encryption Key: [Empty field]
  - Message Authenticator Code Key: [Empty field]
  - Key Input Format:  ASCII  Hexadecimal
- Authenticate Using: RADIUS (Cisco Airespace)
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure):
- Log Update/Watchdog Packets from this AAA Client:
- Log RADIUS Tunneling Packets from this AAA Client:
- Replace RADIUS Port info with Username from this AAA Client:
- Match Framed-IP-Address with user IP address for accounting packets from this AAA Client:

At the bottom of the dialog box, there are three buttons: Submit, Submit + Apply, and Cancel.

该共享密钥必须与您在无线控制器上配置的共享密钥相同。

4. 从身份验证使用下拉式菜单中选择 RADIUS (Cisco Airespace)。
5. 点击 Submit + Restart，以保存配置。

## 配置用户和其相应的 RADIUS IETF 属性。

为了通过 RADIUS 服务器验证用户登录和管理无线控制器，你必须将用户添加到 RADIUS 数据库，还要根据用户的权限将 IETF RADIUS 属性集服务类型 (Service-Type) 设置为适当的值。

\*对于读写权限用户，设置服务类型为 Administrative。

\*对于只读权限用户，设置服务类型为 NAS-Prompt。

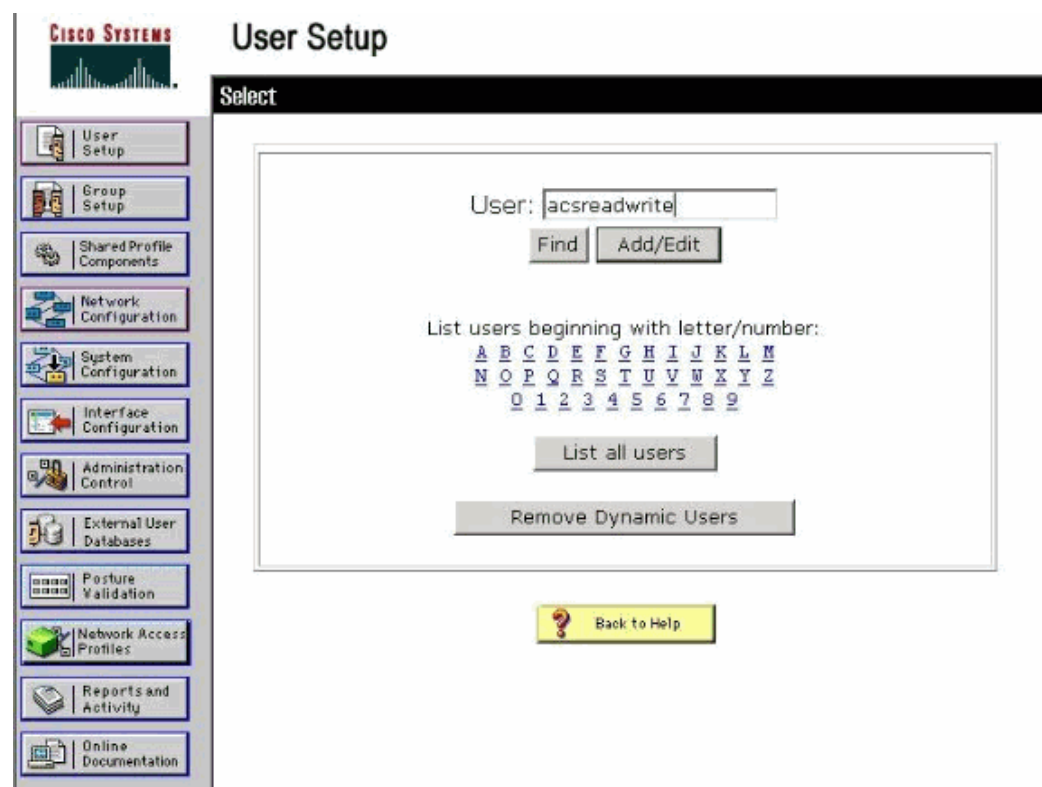
## 配置具有读写访问权限的用户

第一个例子显示了一个具有完全访问无线控制器的用户配置。当该用户试图登录到无线控制器，经过 RADIUS 服务器认证后该用户具有完全管理权限。

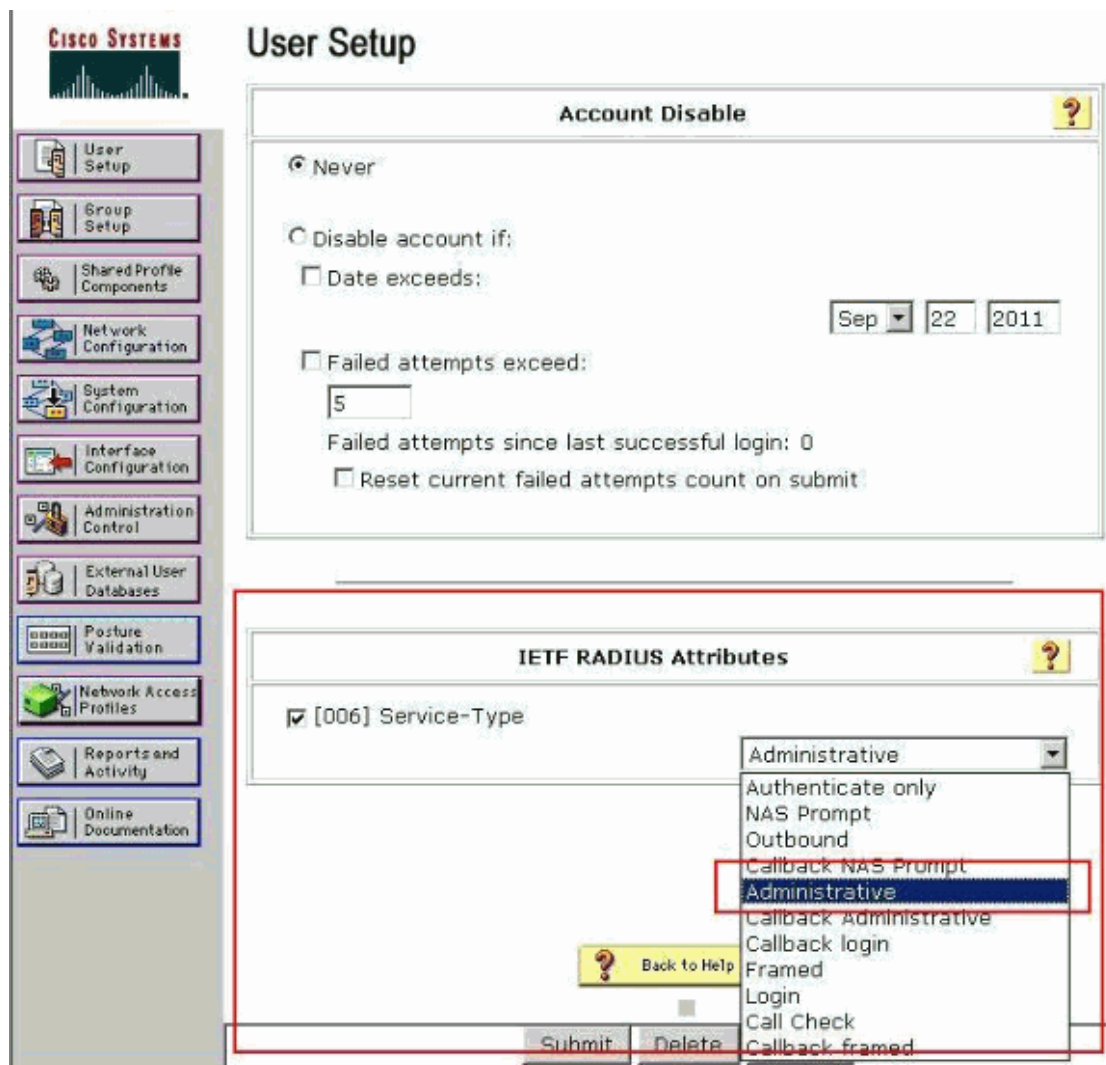
在这个例子中，用户名和密码是 acsreadwrite。在思科 Secure ACS 上完成下列配置步骤。

1.从 ACS 的 GUI 界面，单击用户设置。

2.键入用户名。



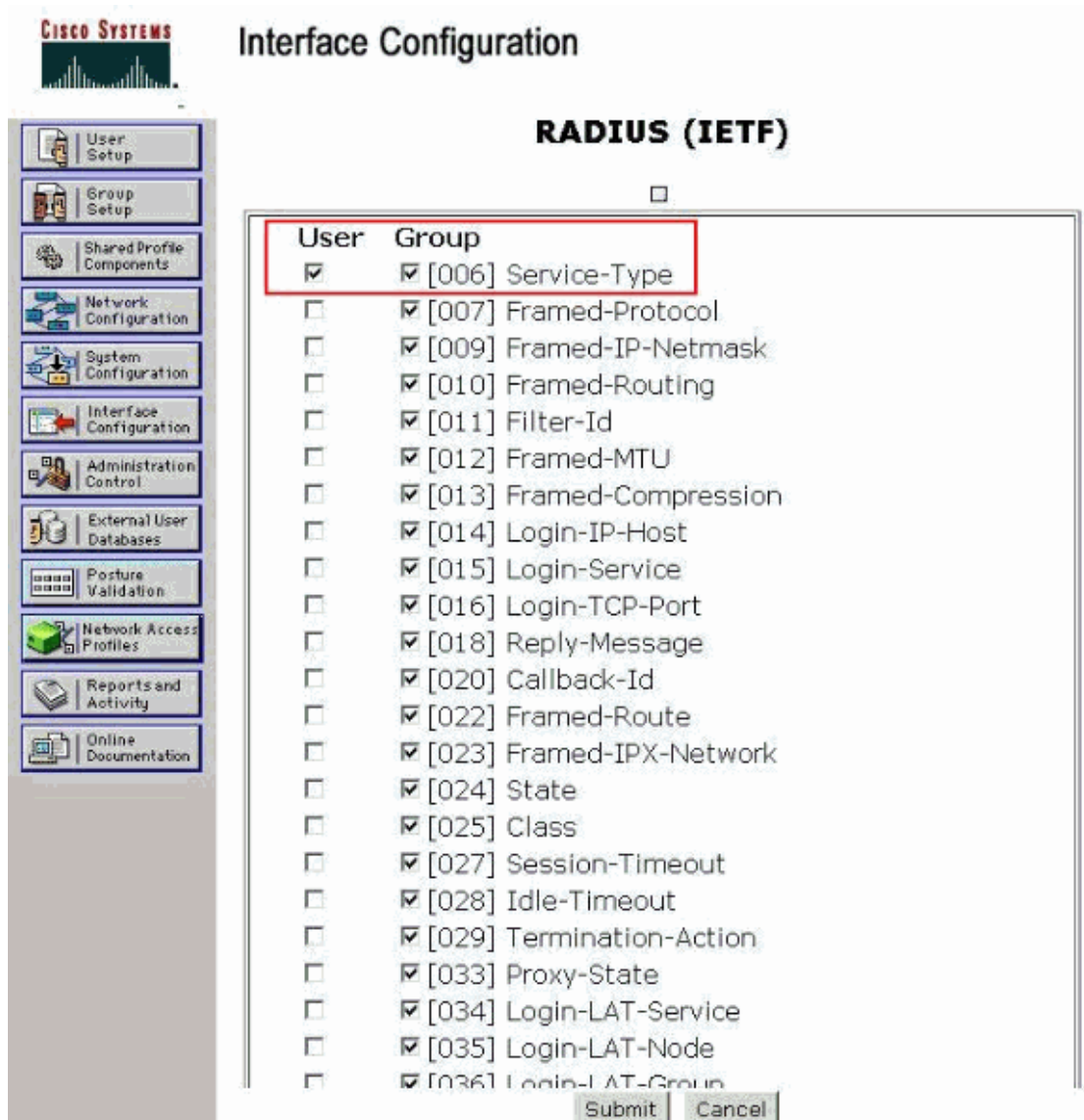
- 3.单击添加/编辑到用户编辑页面。
- 4.在用户编辑页面输入真实姓名，说明和该用户的密码。
- 5.向下滚动到 IETF RADIUS 属性设置并选择服务类型属性 。
- 6.因为在这个例子中用户 `acsreadwrite` 需要给予完全访问权限，从下拉菜单选择 `Administrative` 并点击提交。这将确保这个特定的用户有读写访问无线控制器的权限。



有时候，该服务类型的属性在用户设置下不可见。这时完成下列步骤使其可见。

- 1.从 ACS 的 GUI 界面选择 `Interface Configuration > RADIUS (IETF)` 以便设置用户配置窗口中的 IETF 属性。
- 2.从 RADIUS (IETF) 的设置页面，你可以配置 IETF 的属性，根据用户或组设置可见。对于此配置，选择服务类型和用户列然后点击提交。如下图所示。





注：此示例按照每用户的基础上进行身份验证。您也可以在一组特定的用户的基础上执行认证。在这种情况下选择组复选框使这一属性在组设置下是可见的。

注：此外，如果验证是在一个组的基础上，你需要将用户分配到一个特定的组，并配置该组的 IETF 属性为用户提供访问权限。

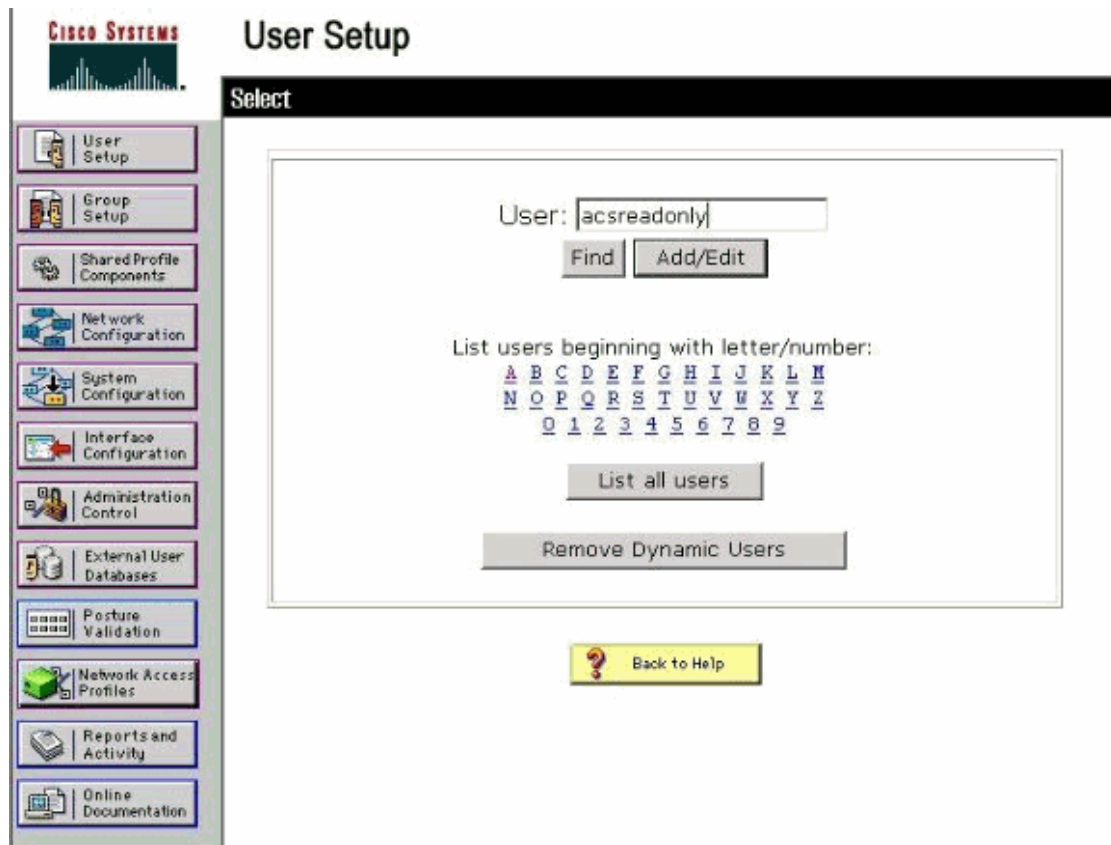
## 配置只读访问用户

本例子显示了一个具有只读访问无线控制器的用户配置。当该用户试图登录到无线控制器，经过 RADIUS 服务器认证后该用户具有只读访问管理权限。

在这个例子中，用户名和密码是 acsreadonly。在思科 Secure ACS 上完成下列配置步骤。



- 1.从 ACS 的 GUI 界面，单击用户设置。
- 2.键入用户名并单击添加/编辑到用户编辑页面。



- 3.在用户编辑页面输入真实姓名，说明和该用户的密码。

**CISCO SYSTEMS**

## User Setup

Edit

### User: acsreadonly (New User)

Account Disabled

#### Supplementary User Info

Real Name:

Description:

#### User Setup

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password:

Confirm Password:

Separate (CHAP/MS-CHAP/ARAP)

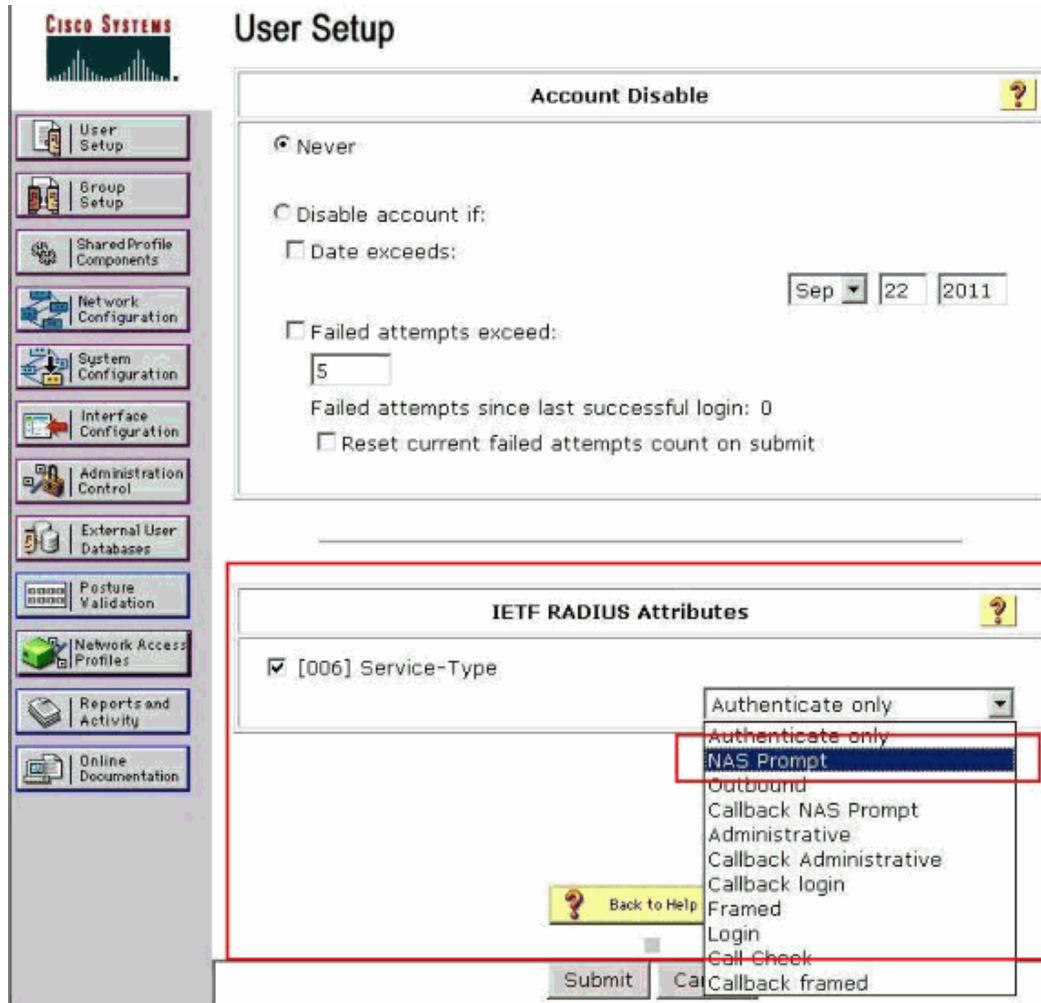
Password:

Confirm Password:

When a token server is used for authentication, supplying a

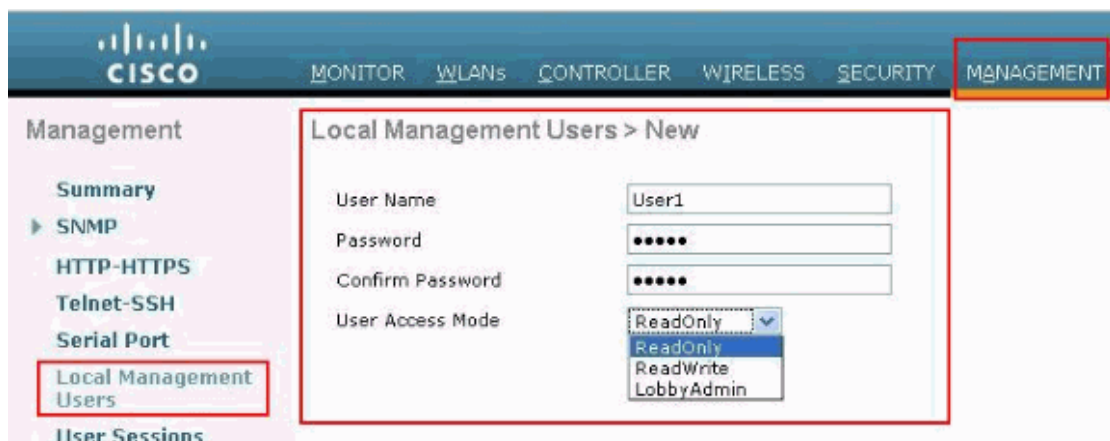
4. 向下滚动到 IETF RADIUS 属性设置并选择服务类型属性。

5. 因为在这个例子中用户 `acsreadonly` 需要给予完全访问权限，从下拉菜单选择 `NAS Prompt` 并点击提交。这将确保这个特定的用户有只读访问无线控制器的权限。



## 无线控制器本地管理用户

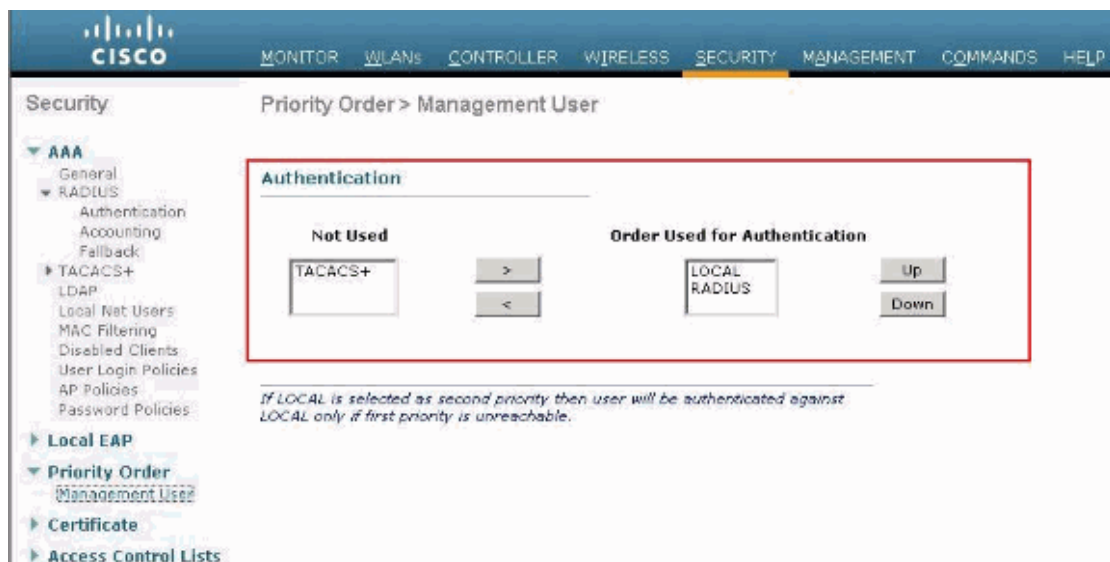
您也可以在无线控制器上配置本地管理用户。这可以从无线控制器的图形用户界面 Management > Local Management Users 完成。



假设无线控制器被配置为既有本地管理用户又启用了 RADIUS 服务器的管理复选框。这时默认情况下，当用户试图登录到无线控制器，无线控制器的行为方式如下：

- 1.无线控制器首先着眼于本地管理用户来验证用户。如果用户在其本地列表中存在，那么它允许对该用户的身份验证。如果此用户没有在本机，那么它将查询 RADIUS 服务器。
- 2.如果本地和 RADIUS 服务器存在相同的用户，但具有不同的访问权限，那么无线控制器对用户进行身份验证采用本地指定的权限。换句话说，在无线控制器上的本地配置总是比 RADIUS 服务器优先。

可以改变无线控制器上管理用户认证的顺序。为了做到这一点，从无线控制器上的安全性页面，单击 **Priority Order > Management User**。从这里你可以指定身份验证的顺序。



注：如果第二优先选择本地，那么只有当第一优先的 RADIUS/TACACS 不可用时才会采用本地认证。

## 验证

为了验证您的配置是否正常工作，通过 CLI 或 GUI（HTTP/HTTPS）模式访问无线控制器。当出现登录提示键入配置在思科 Secure ACS 的用户名和密码。

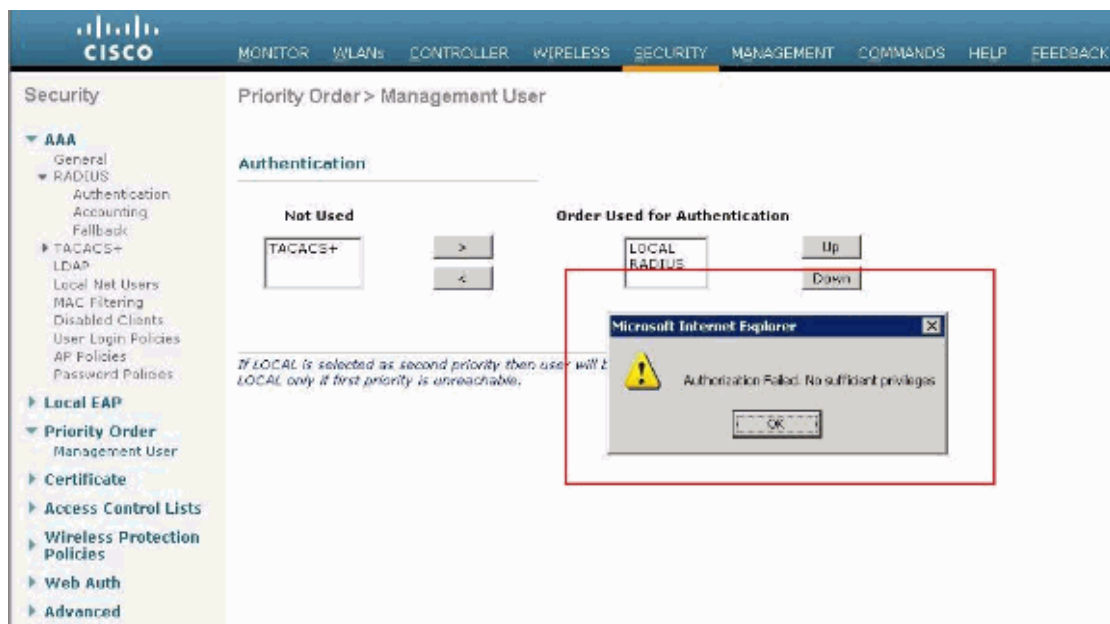
如果你有正确的配置，身份验证成功，你可以进入无线控制器。您还可以确认经过身份验证的用户是否具备 ACS 指定的权限。

读写访问的用户具备配置权限。例如，读写权限用户可以在 WLAN 页面下创建新的 WLAN。

如下图所示。



当一个只读权限的用户试图改变无线控制器上的配置时，可以看到下图的提示消息。



这些访问的限制，也可以通过无线控制器的 CLI 验证。下面的输出显示了一个例子。

(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.

在无线控制器 CLI 输入? 时可以显示当前用户可用的命令列表。请您注意 config 命令在这个例子的输出中不存在。这说明了一个只读用户没有权利在无线控制器上做任何配置。然而，读写用户有权限对无线控制器（GUI 和 CLI 模式）做配置。

注：即使一个用户已经通过了 RADIUS 服务器进行身份验证，当你在网页浏览无线控制器页

面时，HTTP [S]服务器每次仍然要对客户进行完整的验证。你是会在每一页上显示认证提示的唯一原因是您的浏览器具备缓存并将重复使用您的用户凭据进行验证。

## 故障排查

有某些情况下，当无线控制器管理用户通过 ACS 认证，认证成功完成，你看不到任何无线控制器上的授权错误，但会提示用户再次进行身份验证。

在这种情况下，你无法解释什么是错的，为什么用户不能登录到无线控制器，此时使用 `debug aaa events enable` 命令进行排查。

一个可能的原因是 ACS 没有为特定的用户或组配置传输服务类型属性，即使用户名和密码是正确的配置。

如下 `debug aaa events enable` 的命令输出没有显示用户所需的属性（在这个例子中，服务类型属性），即使从 AAA 服务器已经发送回了一个 Access-Accept 消息。

```
(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
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
Mon Aug 13 20:14:33 2011: Packet contains 0 AVPs:
```

通过上面的命令输出，你会看到访问接受消息从 RADIUS 服务器成功接收，但服务类型属性没有传递到无线控制器。这是因为特定用户没有在 ACS 上配置此属性。

根据用户的权限对思科 Secure ACS 进行返回服务类型属性（Administrative 或 NAS-Prompt）

配置后。第二个例子的命令输出显示如下。

```
(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
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
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
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/acserver (36 bytes)
```

你可以看到在这个例子的输出中服务类型属性传递到了无线控制器。

原文链接: [http://www.cisco.com/en/US/tech/tk722/tk809/technologies\\_configuration\\_example09186a0080782507.shtml](http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a0080782507.shtml)

翻译人: 谢清

译于 2012 年 12 月