# 每个用户ACL与无线局域网控制器和Cisco Secure ACS配置示例

## 目录

## 简介

本文档通过示例说明如何在WLC上创建访问控制列表(ACL)，并根据RADIUS授权将其应用于用户。

## 先决条件

### 要求

尝试进行此配置之前，请确保满足以下要求：

- 有关如何配置Cisco Secure ACS服务器以验证无线客户端的基本知识
- 了解Cisco Aironet轻量接入点(LAP)和思科无线局域网控制器(WLC)的配置
- Cisco Unified无线安全解决方法知识

## 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5.0.148.0的思科4400系列无线LAN控制器
- 思科Aironet 1231系列轻量接入点(LAP)
- 运行版本3.6的思科Aironet 802.11 a/b/g思科无线局域网客户端适配器
- Cisco Aironet Desktop Utility 版本 3.6
- Cisco Secure ACS 服务器版本 4.1
- 运行IOS®版本12.4(11)T的Cisco 2800$^{\text{系列}}$集成多业务路由器
- 运行版本12.0(5)WC3b的Cisco Catalyst 2900XL系列交换机

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

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

# 背景信息

每用户访问控制列表(ACL)是思科身份网络的一部分。思科无线LAN解决方案支持身份网络，它允许网络通告单个SSID，同时允许特定用户根据其用户配置文件继承不同的策略。

每个用户的ACL功能提供了根据RADIUS授权将无线局域网控制器上配置的ACL应用于用户的功能。这通过Airespace-ACL-Name供应商特定属性(VSA)实现。

此属性指示要应用于客户端的ACL名称。当ACL属性存在于RADIUS Access Accept中时，系统在对客户端站进行身份验证后将ACL-Name应用到客户端站。这撤销的所有ACL都被分配到接口上。它会忽略分配的接口ACL并应用新接口ACL。

ACL-Name属性格式的摘要如下所示。字段从左到右传输

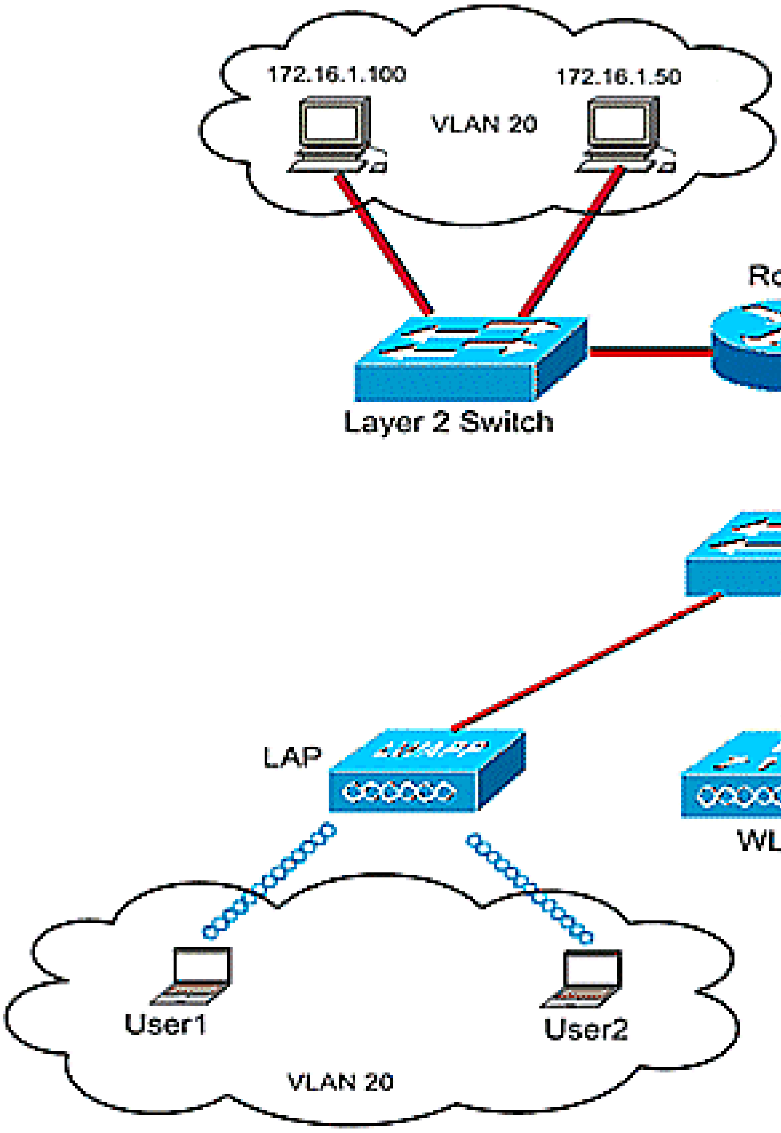
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)           |  Vendor type  | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        ACL Name...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
• Type - 26 for Vendor-Specific
• Length - >7
• Vendor-Id - 14179
• Vendor type - 6
• Vendor length - >0
• Value - A string that includes the name of the ACL to use for the client.
   The string is case sensitive.
```

有关Cisco Unified Wireless Network Identity Networking的详细信息，请参阅文档配置安全解决方案的配置身份网络部分。

## 网络图

本文档使用以下网络设置：

在此设置中，无线LAN控制器WLC和LAP用于向部门A和部门B的用户提供无线服务。所有无线用户都使用通用WLAN(SSID)Office访问网络，并位于VLAN Office-VLAN中。



思科安全ACS服务器用于对无线用户进行身份验证。EAP身份验证用于对用户进行身份验证。WLC、LAP和Cisco Secure ACS服务器与第2层交换机连接，如图所示。

如图所示，路由器R1通过第2层交换机连接有线端的服务器。路由器R1也充当DHCP服务器，从子网172.16.0.0/16为无线客户端提供IP地址。

您需要配置设备，以便发生以下情况：

A部门的用户1只能访问服务器172.16.1.100

B部门的用户2只能访问服务器172.16.1.50

为此，您需要在WLC上创建2个ACL:一个用于User1，另一个用于User2。创建ACL后，您需要配置Cisco Secure ACS服务器，以在无线用户成功进行身份验证后将ACL名称属性返回到WLC。然后，WLC将ACL应用到用户，因此网络会根据用户配置文件进行限制。

**注意：**本文档使用LEAP身份验证对用户进行身份验证。Cisco LEAP易受字典攻击。在实时网络中，应使用更安全的身份验证方法，如EAP FAST。由于本文档的重点是说明如何配置每用户ACL功能，因此使用LEAP是为了简单起见。

下一节提供配置此设置设备的分步说明。

# 配置

在配置每用户ACL功能之前，必须配置WLC以执行基本操作，并将LAP注册到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。如果您是新用户，尝试设置WLC以进行LAP的基本操作，请参阅轻量AP(LAP)注册到无线LAN控制器(WLC)。

注册LAP后，请完成以下步骤以配置此设置的设备：

1. 配置无线局域网控制器。
2. 配置Cisco Secure ACS服务器。
3. 验证配置。

**注意：**本文档讨论无线端所需的配置。本文档假设有线配置已部署。

# 配置无线局域网控制器

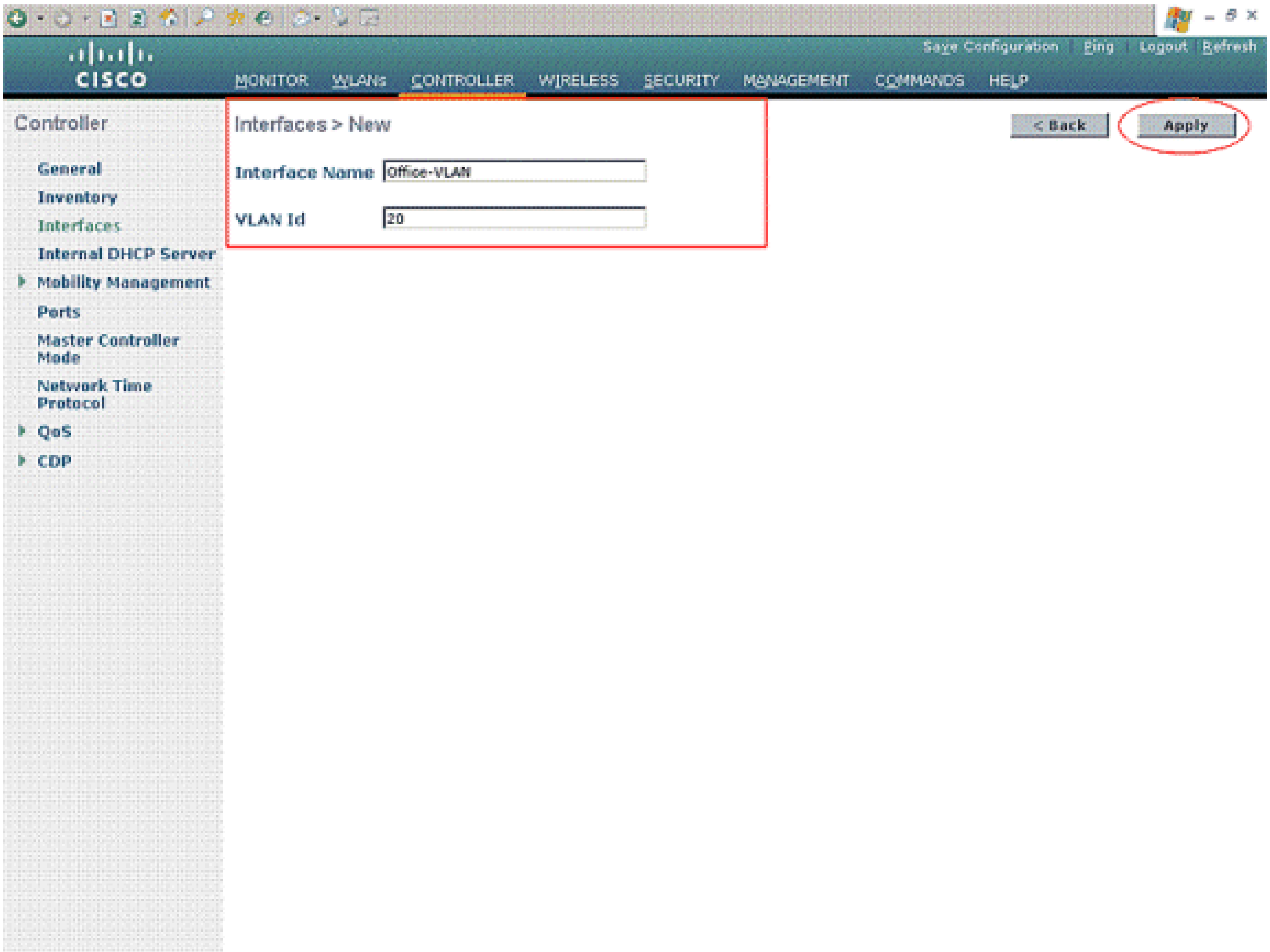
在无线LAN控制器上，您需要执行以下操作：

- 为无线用户创建VLAN。
- 配置WLC以使用思科安全ACS对无线用户进行身份验证。
- 为无线用户创建新的WLAN。
- 定义无线用户的ACL。

## 为无线用户创建VLAN

要为无线用户创建VLAN，请完成以下步骤。

1. 转到 WLC GUI，然后选择 **Controller > 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。
2. 单击 **New 创建新的动态接口。**
3. 在“Interfaces”>“New”窗口中的“Interface Name”和“VLAN ID”中输入相应信息。然后单击 Apply。在本例中，动态接口命名为Office-VLAN，VLAN ID分配为20。

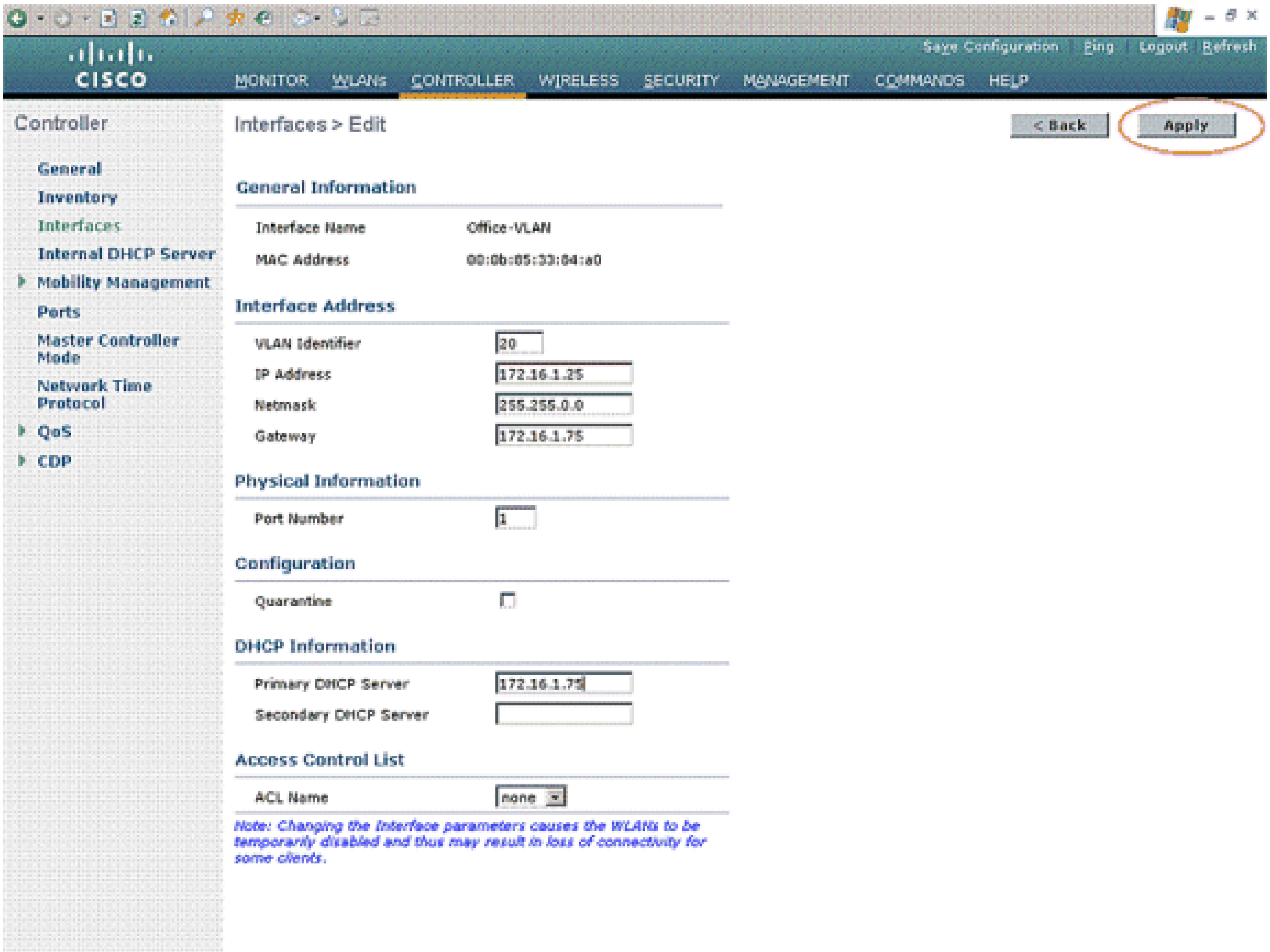


Interfaces > New

Interface Name Office-VLAN

VLAN Id 20

4. 在 **Interfaces > Edit 窗口中，输入动态接口的 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**。



Interfaces > Edit

General Information

Interface Name: Office-VLAN

MAC Address: 00:0b:85:33:84:a0

Interface Address

VLAN Identifier: 20

IP Address: 172.16.1.25

Netmask: 255.255.0.0

Gateway: 172.16.1.75

Physical Information

Port Number: 1

Configuration

Quarantine: □

DHCP Information

Primary DHCP Server: 172.16.1.75

Secondary DHCP Server:

Access Control List

ACL Name: none

*Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.*

在本例中，这些参数用于Office-VLAN接口：

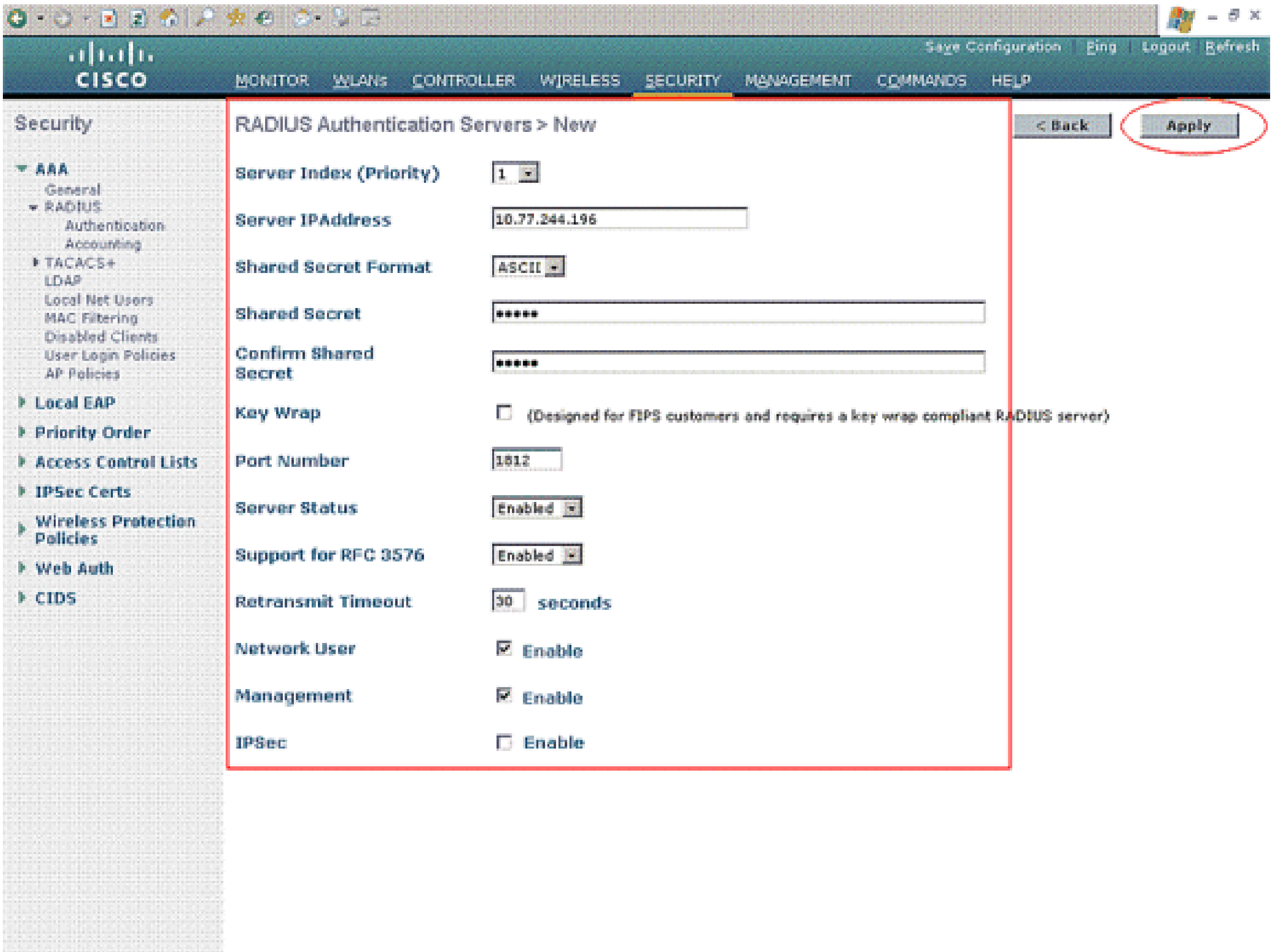
```
Office-VLAN
IP address: 172.16.1.25
Netmask: 255.255.0.0
Default gateway: 172.16.1.75 (sub-interface on Router R1)
Port on WLC: 1
DHCP server: 172.16.1.75
```

## 将WLC配置为使用Cisco Secure ACS进行身份验证

需要配置WLC，以将用户凭证转发到外部RADIUS服务器（本例中为Cisco Secure ACS）。 然后，RADIUS服务器验证用户凭证并在无线用户成功进行身份验证后将ACL名称属性返回给WLC。

要为RADIUS服务器配置WLC，请完成以下步骤：

1. 从控制器的 GUI 中选择**安全性和“RADIUS 身份验证”，以便显示“RADIUS 身份验证服务器”页。**然后，单击**新建定义 RADIUS 服务器。**
2. 在 **RADIUS 身份验证服务器 > 新建页中定义 RADIUS 服务器参数。**这些参数包括 RADIUS 服务器的 IP 地址、共享密钥、端口号和服务器状态。



RADIUS Authentication Servers > New

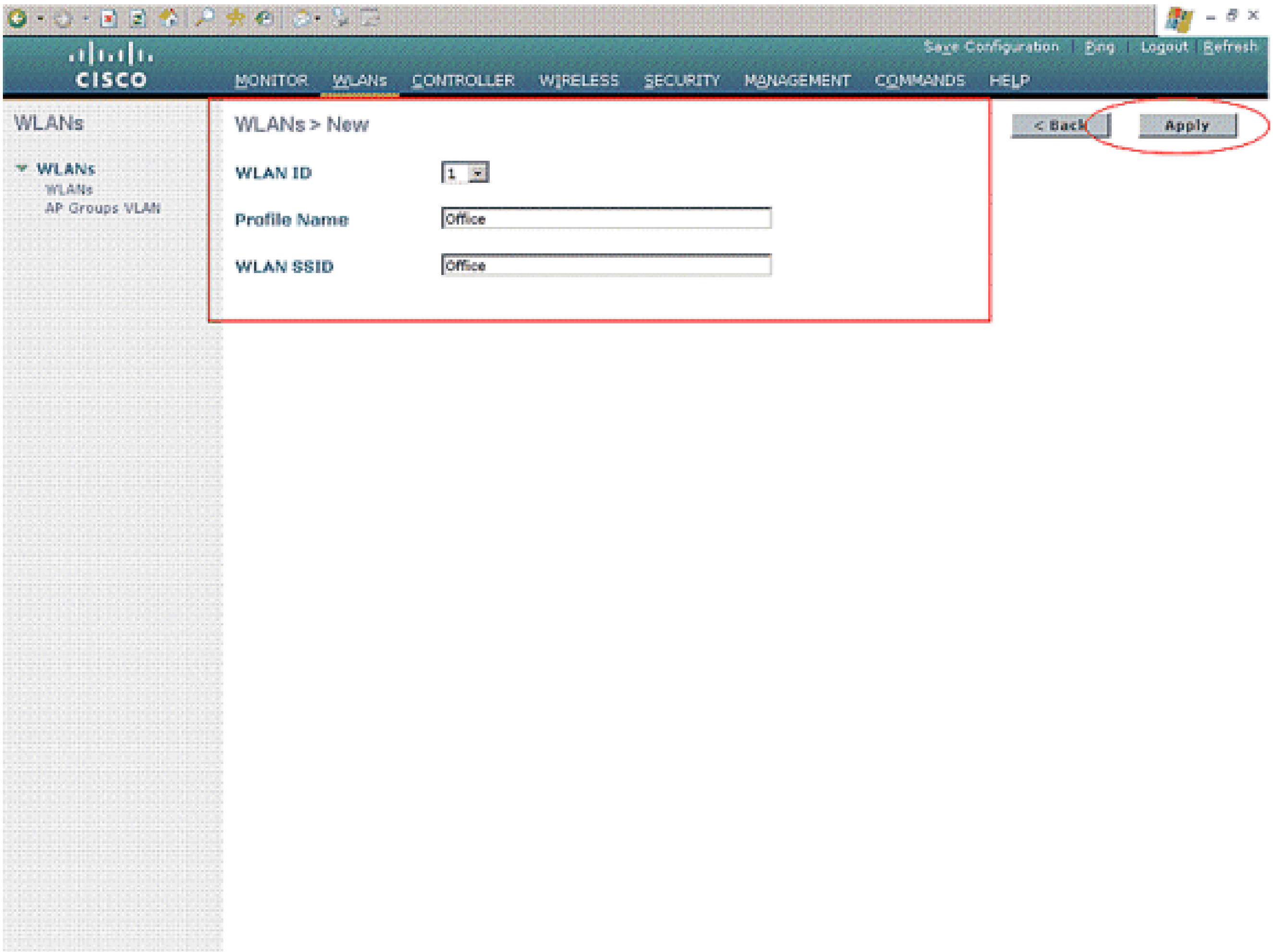
| | |
|---|---|
| Server Index (Priority) | 1 |
| Server IPAddress | 10.77.244.196 |
| Shared Secret Format | ASCII |
| Shared Secret | ***** |
| Confirm Shared Secret | ***** |
| Key Wrap | □ (Designed for FIPS customers and requires a key wrap compliant RADIUS server) |
| Port Number | 1812 |
| Server Status | Enabled |
| Support for RFC 3576 | Enabled |
| Retransmit Timeout | 30 seconds |
| Network User | ☑ Enable |
| Management | ☑ Enable |
| IPSec | □ Enable |

3. “网络用户”和“管理”复选框决定基于 RADIUS 的身份验证是否适用于管理和网络用户。本示例使用Cisco Secure ACS作为IP地址为10.77.244.196的RADIUS服务器。单击**Apply**。

## 为无线用户创建新的WLAN

接下来，您需要创建无线用户可以连接到的WLAN。要创建新的WLAN，请完成以下步骤：

1. 在无线局域网控制器GUI中，单击**WLANs**。此页列出了控制器上现有的 WLAN。
2. 选择**新建创建新的 WLAN。**输入WLAN的WLAN ID、配置文件名称和WLAN SSID，然后单击**Apply**。对于此设置，请创建WLAN **Office**。



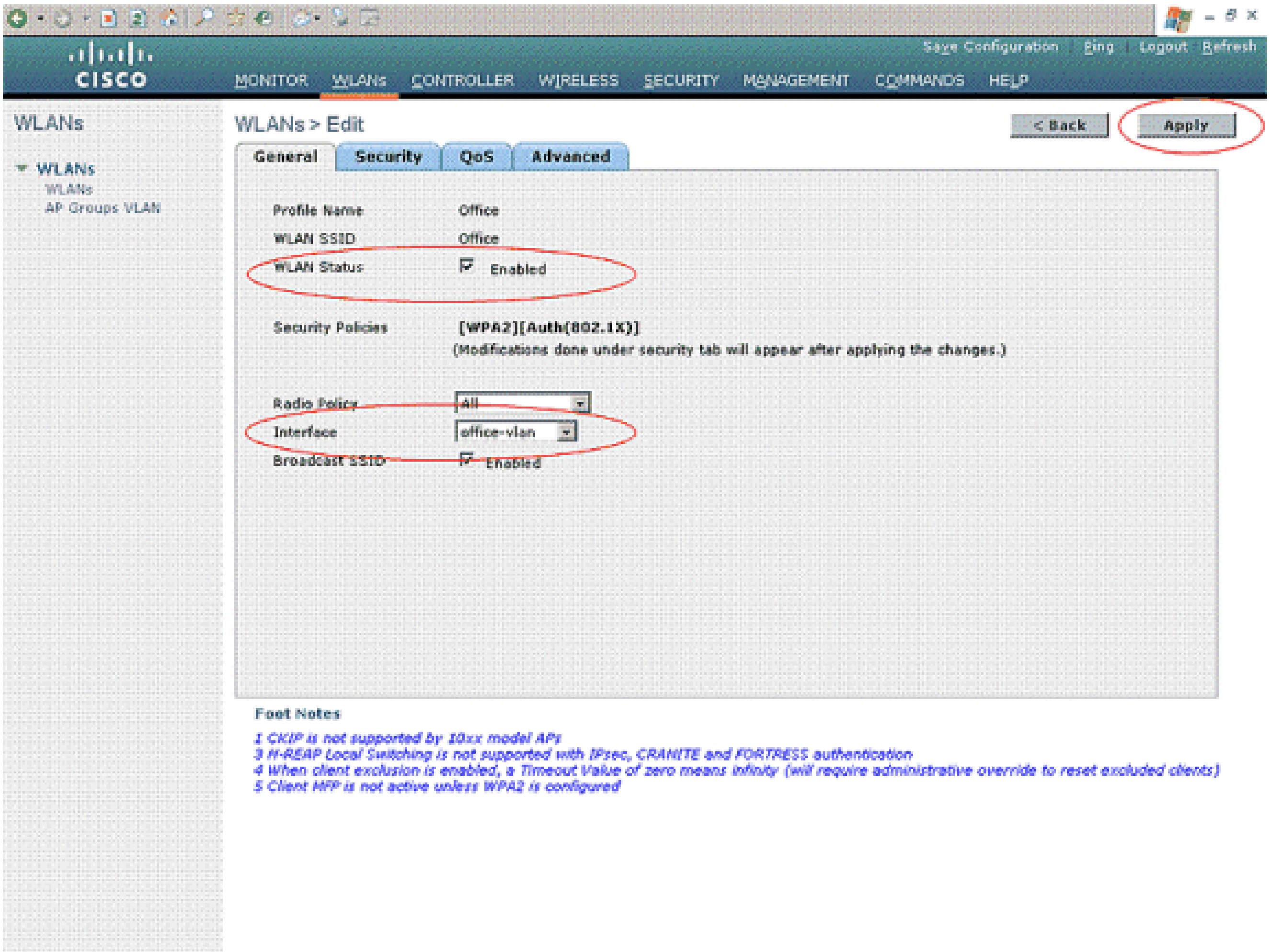
WLANs > New

WLAN ID: 1

Profile Name: Office

WLAN SSID: Office

3. 创建新 WLAN 后，就会显示新 WLAN 的 **WLAN > Edit 页。**在此页中，您可以定义特定于此WLAN的各种参数，包括常规策略、安全、QoS和高级参数。



WLANs > Edit

Profile Name Office

WLAN SSID Office

WLAN Status ☑ Enabled

Security Policies [WPA2][Auth(802.1X)]

(Modifications done under security tab will appear after applying the changes.)

Radio Policy All

Interface office-vlan

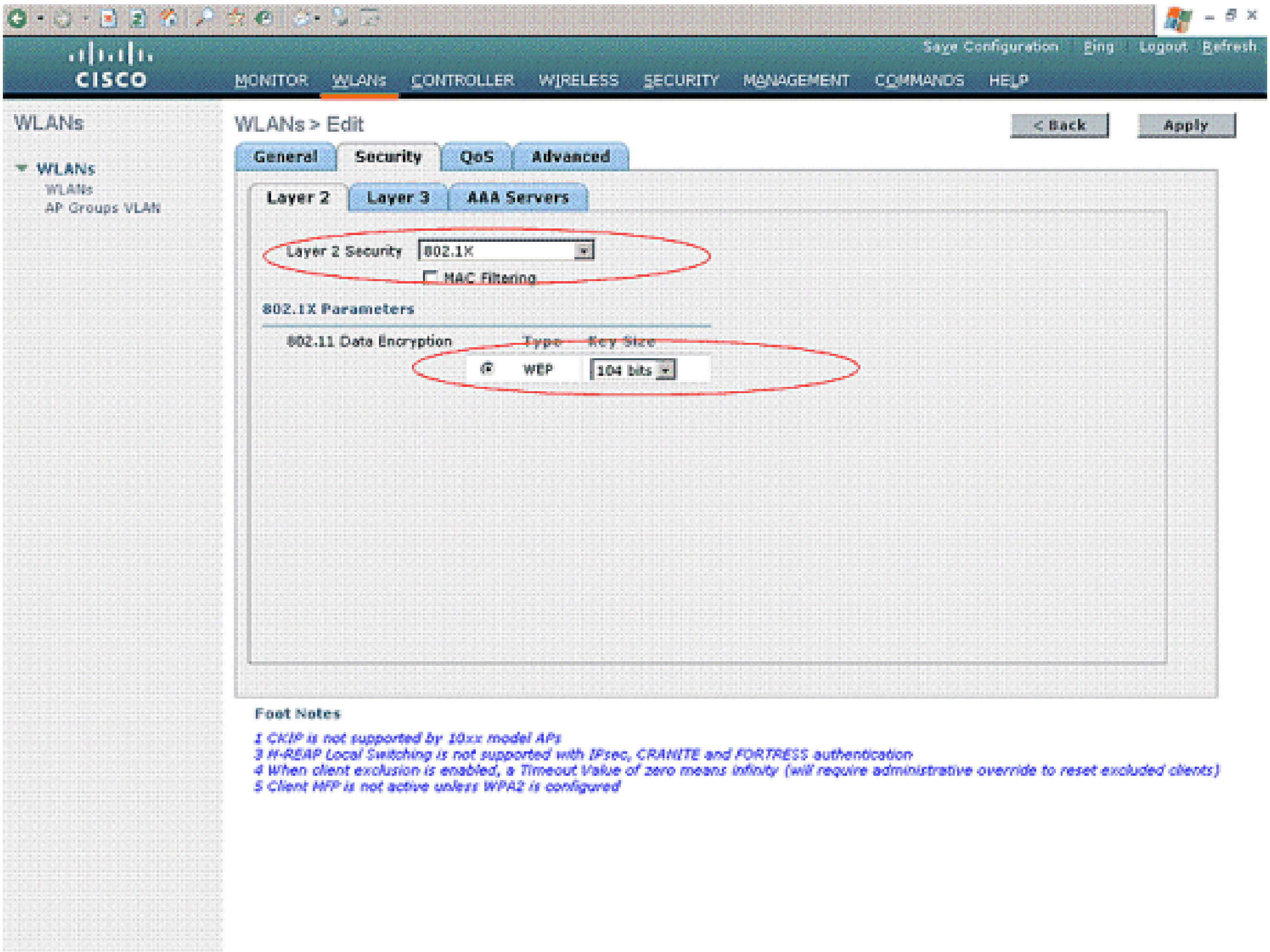
Broadcast SSID ☑ Enabled

Foot Notes

1 CKIP is not supported by 10xx model APs
3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication
4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
5 Client MFP is not active unless WPA2 is configured

选中**General policies**下的**WLAN Status（WLAN状态）以启用WLAN。**从下拉菜单中选择适当的接口。在本例中，使用接口**Office-vlan。**本页中的其他参数可根据WLAN网络的要求进行修改。

4. 选择 **Security** 选项卡。从第**2层安**全下拉菜单中选择802.1x（因为这是LEAP身份验证）。 在802.1x参数下选择适当的WEP密钥大小。



Layer 2 Security 802.1X

□ MAC Filtering

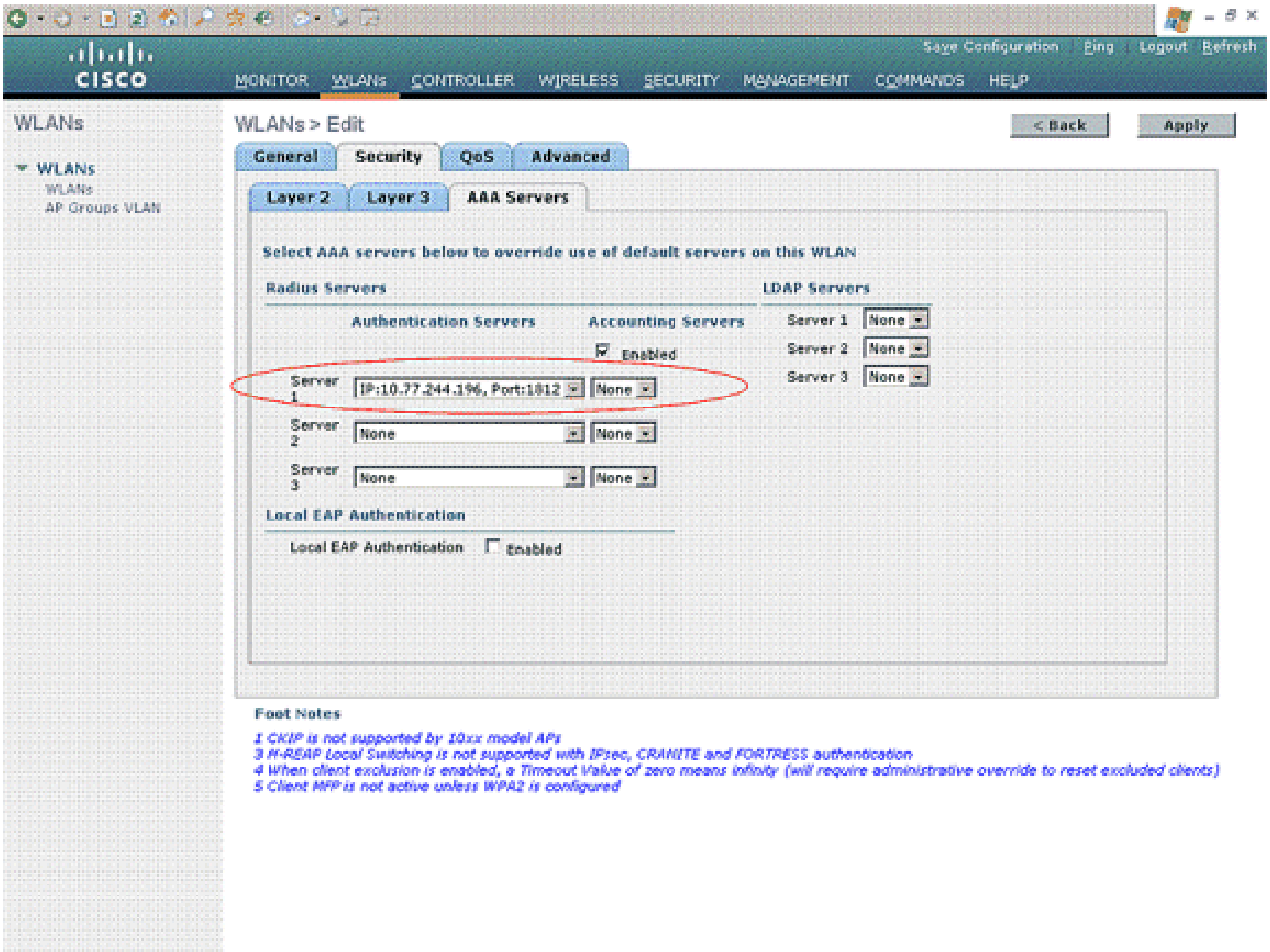
802.1X Parameters

| 802.11 Data Encryption | | Type | Key Size |
|---|---|---|---|
| | ● | WEP | 104 bits |

Foot Notes

1 CKIP is not supported by 10xx model APs
3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication
4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
5 Client MFP is not active unless WPA2 is configured

5. 在Security选项卡下，选择**AAA服**务器子选项卡。选择用于验证无线客户端的AAA服务器。在本示例中，使用ACS服务器10.77.244.196对无线客户端进行身份验证。


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
< Back
Apply
General Security QoS Advanced
Layer 2 Layer 3 AAA Servers

WLANs > Edit

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

| | Authentication Servers | Accounting Servers |
|---|---|---|
| | | ☑ Enabled |
| Server 1 | IP:10.77.244.196, Port:1812 | None |
| Server 2 | None | None |
| Server 3 | None | None |

LDAP Servers

| | |
|---|---|
| Server 1 | None |
| Server 2 | None |
| Server 3 | None |

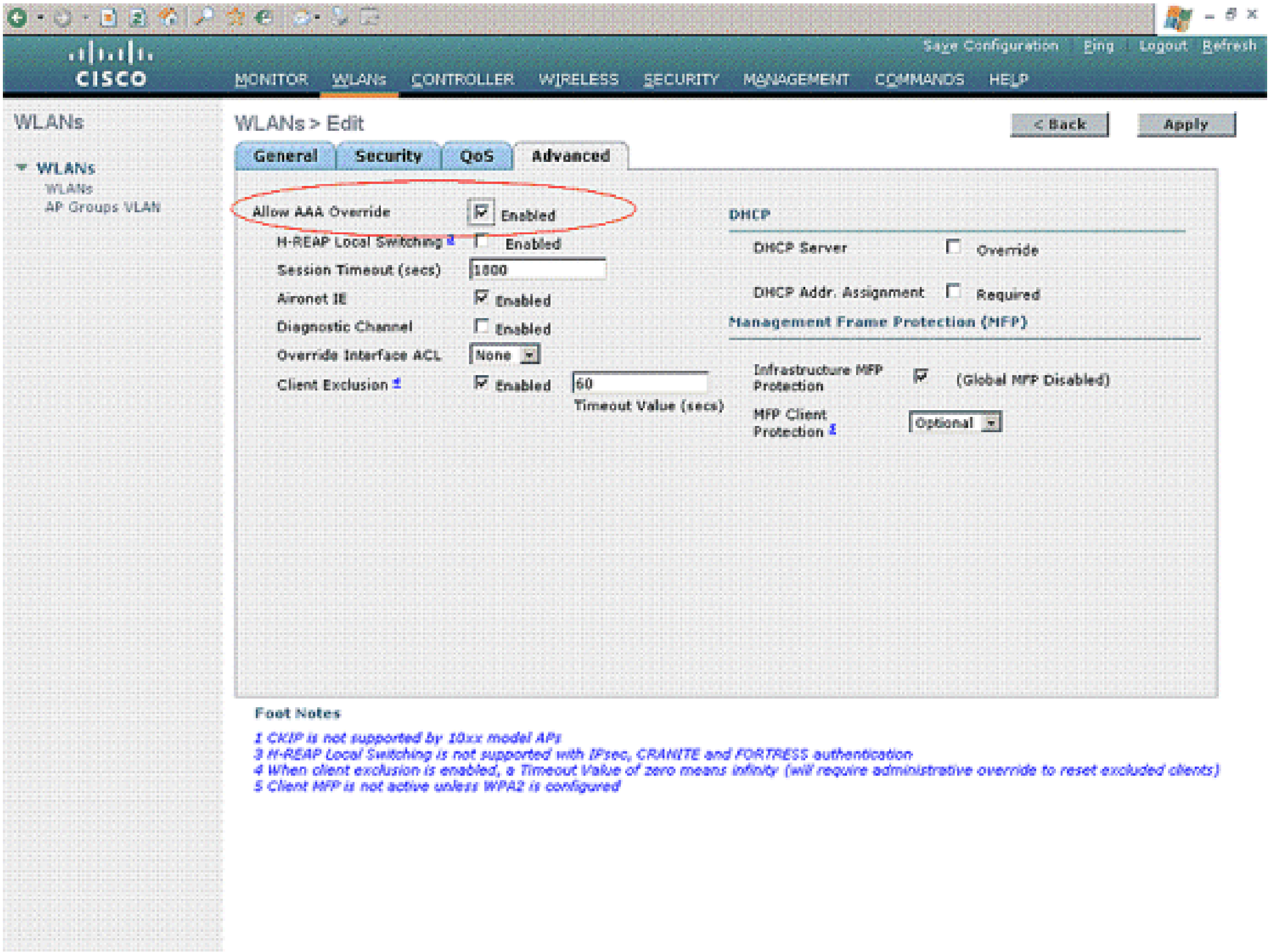
Local EAP Authentication

Local EAP Authentication □ Enabled

Foot Notes

1 CKIP is not supported by 10xx model APs
3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication
4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
5 Client MFP is not active unless WPA2 is configured

6. 选择“高级”选项卡。选中Allow AAA Override以通过无线LAN上的AAA配置用户策略覆盖。


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
< Back
Apply
General Security QoS Advanced

WLANs > Edit

Allow AAA Override ☑ Enabled

H-REAP Local Switching 3 □ Enabled

Session Timeout (secs) 1800

Aironet IE ☑ Enabled

Diagnostic Channel □ Enabled

Override Interface ACL None

Client Exclusion 4 ☑ Enabled 60 Timeout Value (secs)

DHCP

DHCP Server □ Override

DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)

Infrastructure MFP Protection ☑ (Global MFP Disabled)

MFP Client Protection 5 Optional

Foot Notes

1 CKIP is not supported by 10xx model APs
3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication
4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
5 Client MFP is not active unless WPA2 is configured

当AAA覆盖启用，且客户端具有冲突的AAA和思科无线局域网控制器无线局域网身份验证参数时，客户端身份验证由AAA服务器执行。作为此身份验证的一部分，操作系统将客户端从默认的思科无线局域网解决方案无线局域网VLAN移至AAA服务器返回的VLAN，并在思科无线局域网控制器接口配置中预定义VLAN，这仅在配置MAC过滤、802.1X和/或WPA操作时发生。在所有情况下，操作系统还使用QoS、DSCP、802.1p优先级标记值和ACL，只要它们在思科无线局域网控制器接口配置中预定义。

7. 根据网络要求选择其他参数。单击 **Apply**。

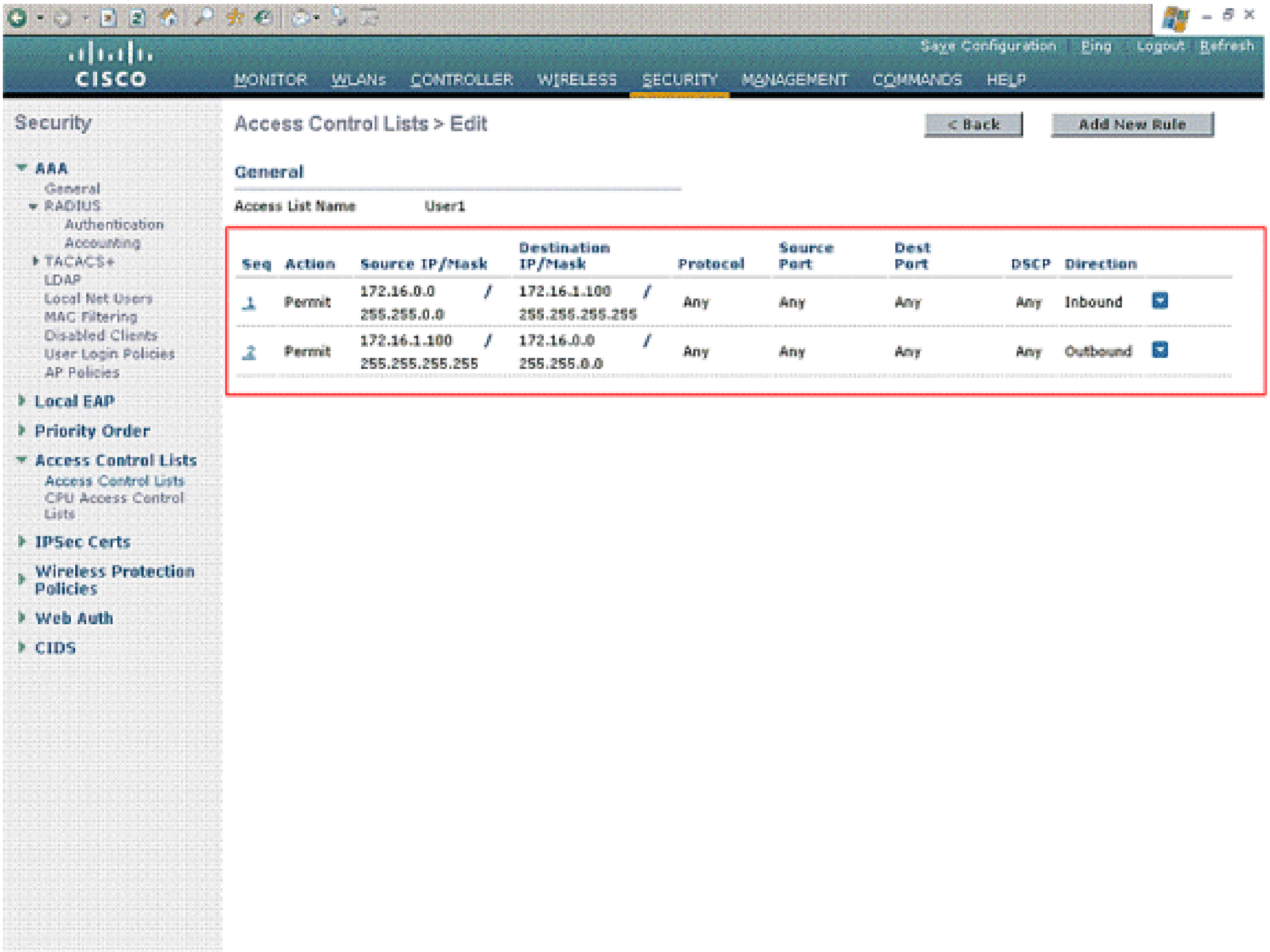
## 为用户定义ACL

您需要为此设置创建两个ACL:

- ACL1:为了仅对服务器172.16.1.100提供对User1的访问
- ACL2:为了仅对服务器172.16.1.50提供对User2的访问

完成以下步骤以在WLC上配置ACL:

1. 从 WLC GUI 中，选择 **Security > Access Control Lists**。出现 Access Control Lists 页。此页列出了在 WLC 上配置的 ACL。您也可以利用它编辑或删除其中任一 ACL。要创建新的 ACL，请单击 **New**。
2. 此页面允许您创建新ACL。输入 ACL 的名称并单击 **Apply**。创建 ACL 后，单击 **Edit 创建 ACL 的规则。**
3. 用户1需要仅能访问服务器172.16.1.100，并且必须拒绝访问所有其他设备。为此，您需要定义这些规则。有关如何在无线LAN控制器上配置ACL的详细信息，请参阅无线局域网控制器上的ACL配置示例。



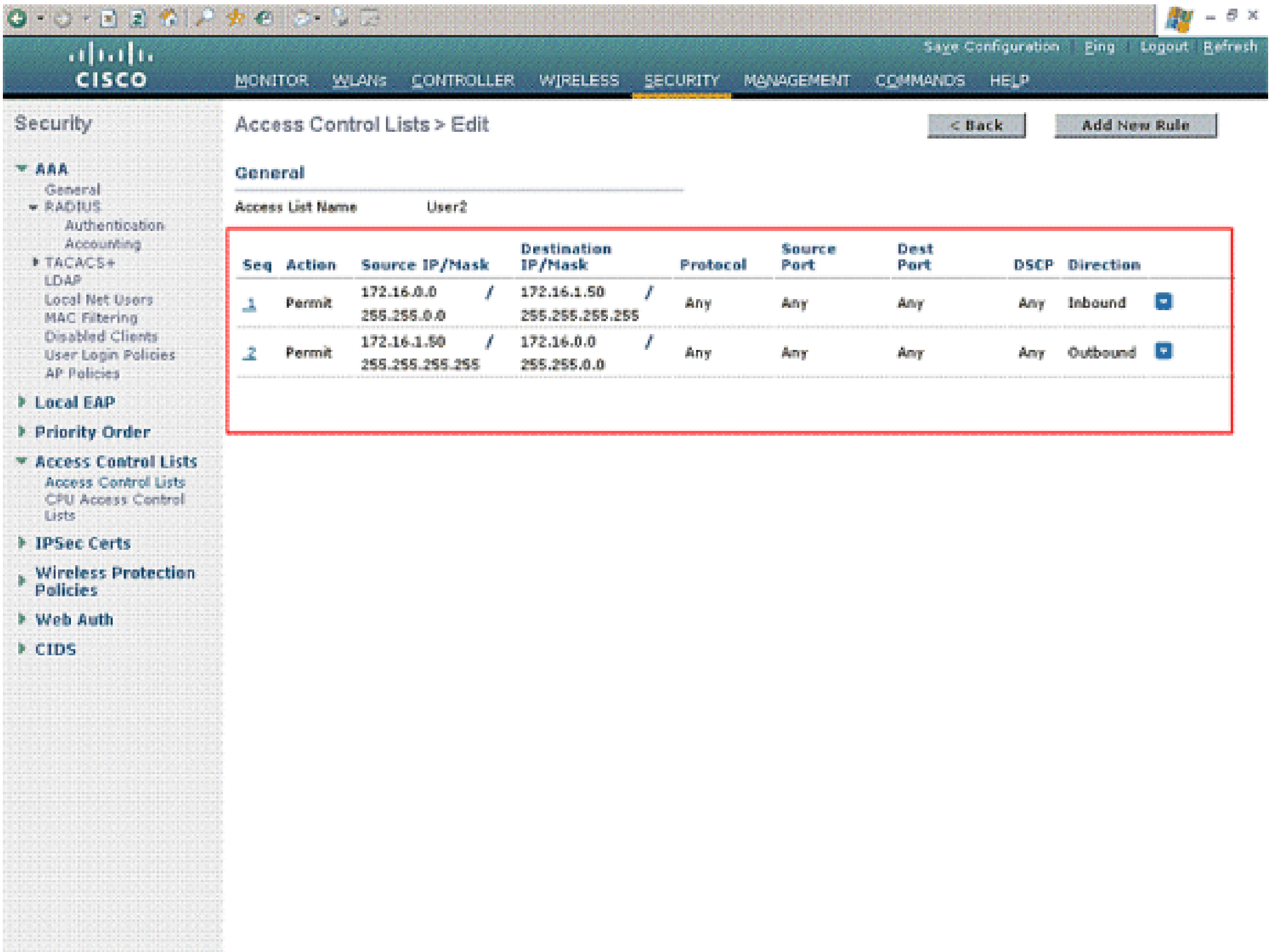
Access Control Lists > Edit

General

Access List Name User1

| Seq | Action | Source IP/Mask | Destination IP/Mask | Protocol | Source Port | Dest Port | DSCP | Direction |
|---|---|---|---|---|---|---|---|---|
| 1 | Permit | 172.16.0.0 / 255.255.0.0 | 172.16.1.100 / 255.255.255.255 | Any | Any | Any | Any | Inbound |
| 2 | Permit | 172.16.1.100 / 255.255.255.255 | 172.16.0.0 / 255.255.0.0 | Any | Any | Any | Any | Outbound |

4. 同样，您需要为User2创建ACL，该ACL仅允许User2访问服务器172.16.1.50。这是User2所需的ACL。



Access Control Lists > Edit

General

Access List Name User2

| Seq | Action | Source IP/Mask | Destination IP/Mask | Protocol | Source Port | Dest Port | DSCP | Direction |
|---|---|---|---|---|---|---|---|---|
| 1 | Permit | 172.16.0.0 / 255.255.0.0 | 172.16.1.50 / 255.255.255.255 | Any | Any | Any | Any | Inbound |
| 2 | Permit | 172.16.1.50 / 255.255.255.255 | 172.16.0.0 / 255.255.0.0 | Any | Any | Any | Any | Outbound |

您现在已为此设置配置了无线局域网控制器。下一步是配置思科安全访问控制服务器以对无线客户端进行身份验证，并在身份验证成功后将ACL名称属性返回到WLC。

# 配置Cisco Secure ACS服务器

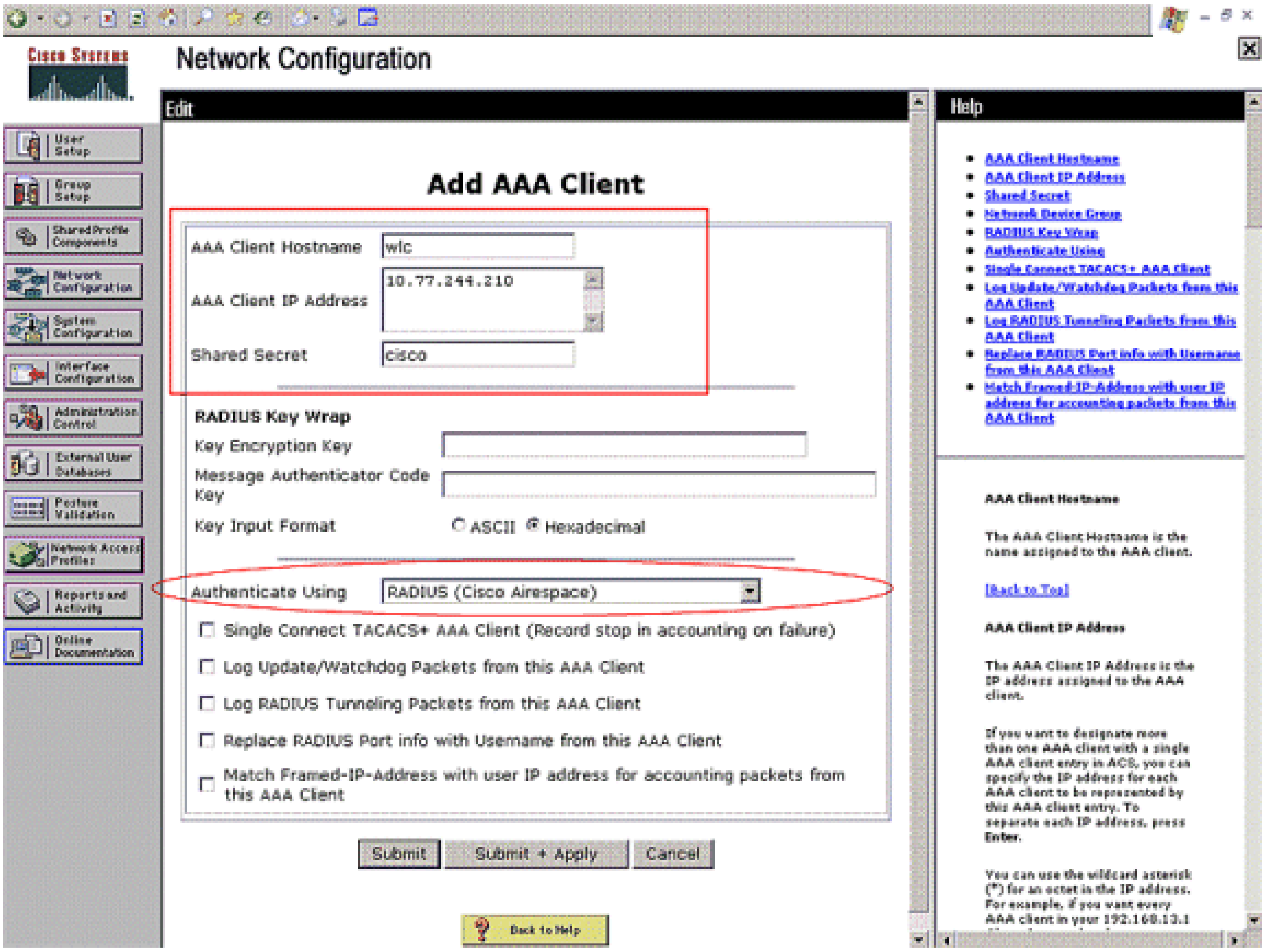
要使思科安全ACS能够对无线客户端进行身份验证，您需要完成以下步骤：

- 在Cisco Secure ACS上将无线局域网控制器配置为AAA客户端。
- 在思科安全ACS上配置用户和用户配置文件。

## 在Cisco Secure ACS上将无线局域网控制器配置为AAA客户端

要将无线局域网控制器配置为思科安全ACS上的AAA客户端，请完成以下步骤：

1. 单击**Network Configuration > Add AAA client**。系统将**显示Add AAA client**页面。在此页中，定义WLC系统名称、管理接口IP地址、共享密钥和使用Radius Airespace进**行身份验证**。示例如下：



Add AAA Client

AAA Client Hostname: wlc

AAA Client IP Address: 10.77.244.210

Shared Secret: cisco

RADIUS Key Wrap

Key Encryption Key:

Message Authenticator Code Key:

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

- AAA Client Hostname
- AAA Client IP Address
- Shared Secret
- Network Device Group
- RADIUS Key Wrap
- Authenticate Using
- Single Connect TACACS+ AAA Client
- 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

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[Back to Top]

AAA Client IP Address

The AAA Client IP Address is the IP address assigned to the AAA client.

If you want to designate more than one AAA client with a single AAA client entry in ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**.

You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1

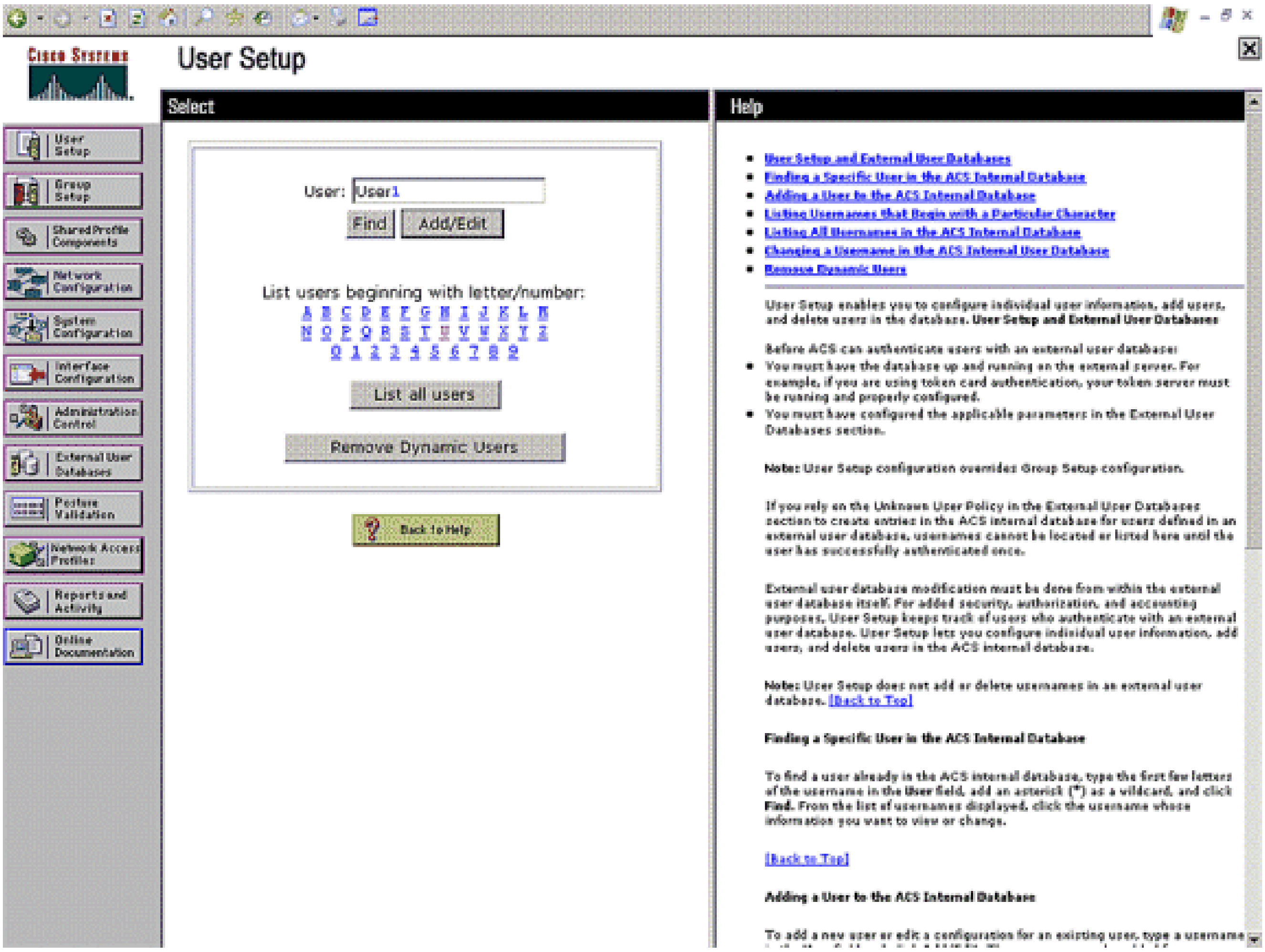
**注意：**在Cisco Secure ACS上配置的共享密钥必须与在WLC上在RADIUS Authentication Servers > New下**配置的共享密钥匹配。**

2. 单击 **Submit+Apply**。

## 在思科安全ACS上配置用户和用户配置文件

要在Cisco Secure ACS上配置用户，请完成以下步骤：

1. 从 ACS GUI 中选择 **User Setup，输入用户名，然后单击 Add/Edit。**在本例中，用户为 **User1**。



User: User1

List users beginning with letter/number:
A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9

- User Setup and External User Databases
- Finding a Specific User in the ACS Internal Database
- Adding a User to the ACS Internal Database
- Listing Usernames that Begin with a Particular Character
- Listing All Usernames in the ACS Internal Database
- Changing a Username in the ACS Internal User Database
- Remove Dynamic Users

User Setup enables you to configure individual user information, add users, and delete users in the database. **User Setup and External User Databases**

Before ACS can authenticate users with an external user database:

- You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
- You must have configured the applicable parameters in the External User Databases section.

**Note:** User Setup configuration overrides Group Setup configuration.

If you rely on the Unknown User Policy in the External User Databases section to create entries in the ACS internal database for users defined in an external user database, usernames cannot be located or listed here until the user has successfully authenticated once.

External user database modification must be done from within the external user database itself. For added security, authorization, and accounting purposes, User Setup keeps track of users who authenticate with an external user database. User Setup lets you configure individual user information, add users, and delete users in the ACS internal database.

**Note:** User Setup does not add or delete usernames in an external user database. [Back to Top]

**Finding a Specific User in the ACS Internal Database**

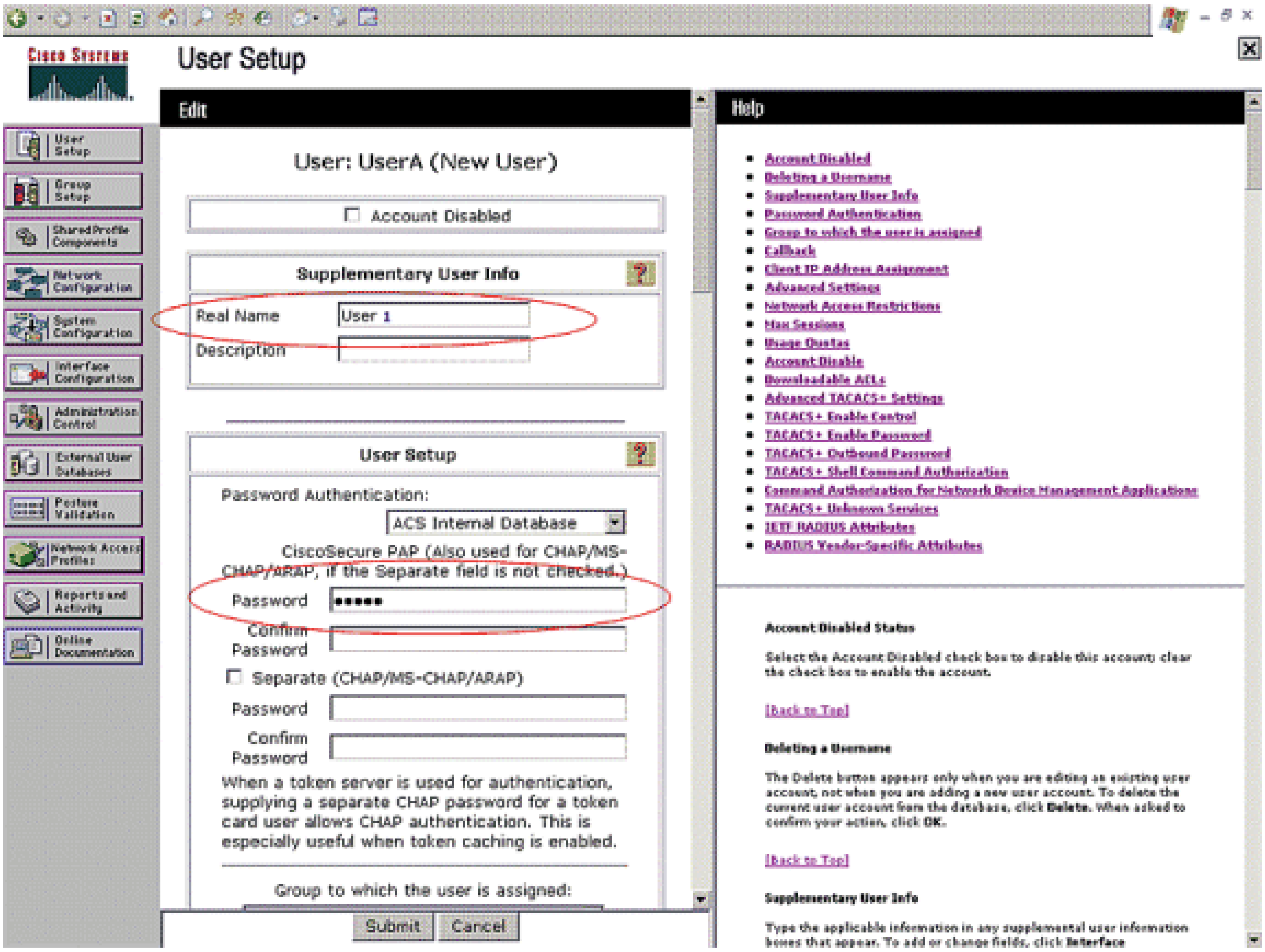
To find a user already in the ACS internal database, type the first few letters of the username in the **User** field, add an asterisk (*) as a wildcard, and click **Find.** From the list of usernames displayed, click the username whose information you want to view or change.

[Back to Top]

**Adding a User to the ACS Internal Database**

To add a new user or edit a configuration for an existing user, type a username

2. 显示“**用户设置**”页时，定义特定于用户的所有参数。在本示例中，配置了用户名、密码、补充用户信息和RADIUS属性，因为您只需要这些参数来进行EAP身份验证。



User: UserA (New User)

□ Account Disabled

Supplementary User Info

Real Name: User 1

Description:

User Setup

Password Authentication:

ACS Internal Database

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 separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

**Account Disabled Status**

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top]

**Deleting a Username**

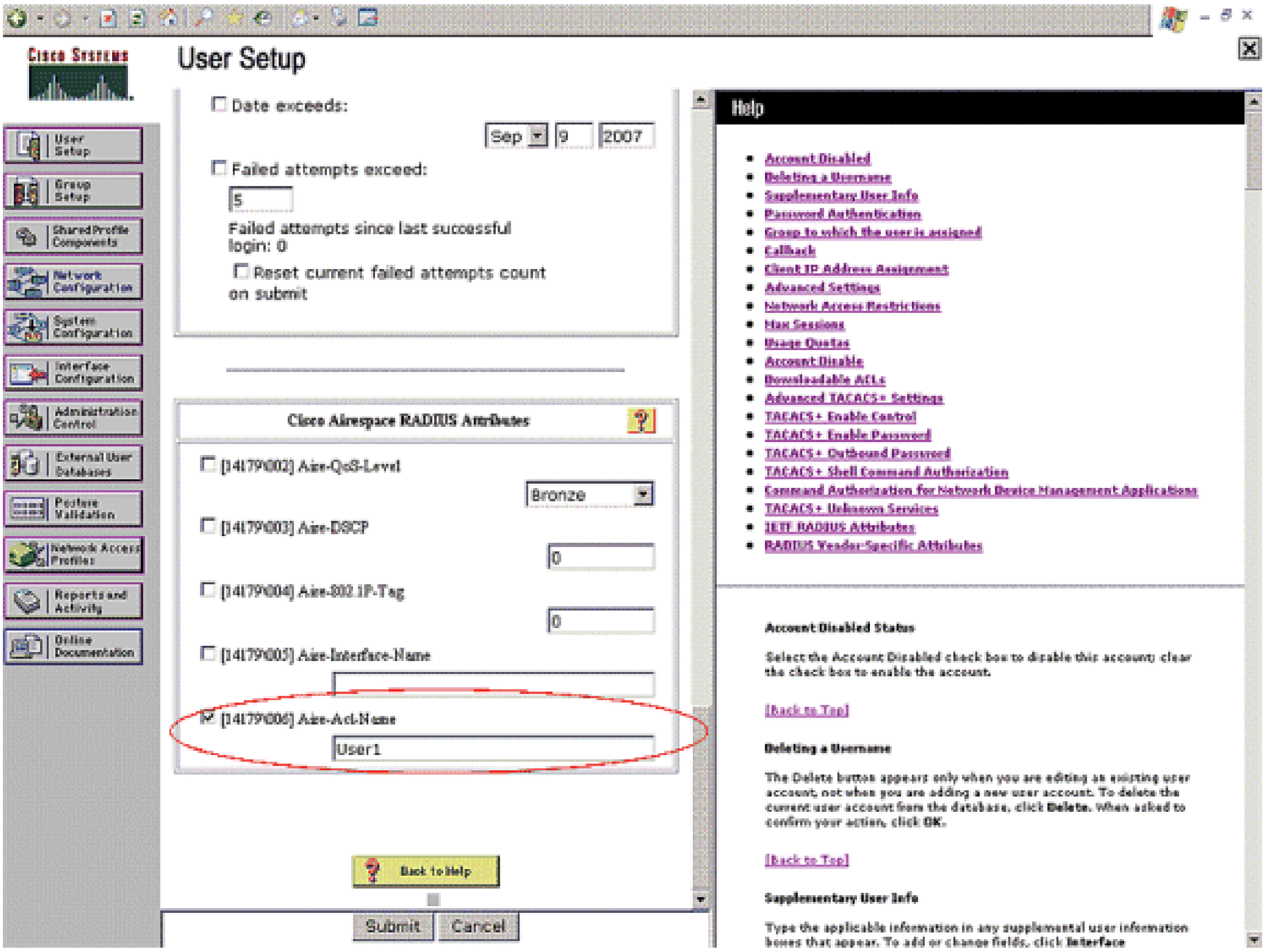
The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click **Delete**. When asked to confirm your action, click **OK**.

[Back to Top]

**Supplementary User Info**

Type the applicable information in any supplemental user information boxes that appear. To add or change fields, click **Interface**

向下滚动，直到您看到特定于用户的Cisco Airespace RADIUS属性。选中**Aire-ACL-Name**，使ACS能够将ACL名称与成功的身份验证响应一起返回到WLC。对于User1，在WLC上创建ACL User1。将ACL名称输入为User1。



□ Date exceeds:

Sep 9 2007

□ Failed attempts exceed:

5

Failed attempts since last successful login: 0

□ Reset current failed attempts count on submit

**Cisco Airespace RADIUS Attributes**

□ [14179\002] Aire-QoS-Level

Bronze

□ [14179\003] Aire-DSCP

0

□ [14179\004] Aire-802.1P-Tag

0

□ [14179\005] Aire-Interface-Name

☑ [14179\006] Aire-Acl-Name

User1

**Help**

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

**Account Disabled Status**

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top]

**Deleting a Username**

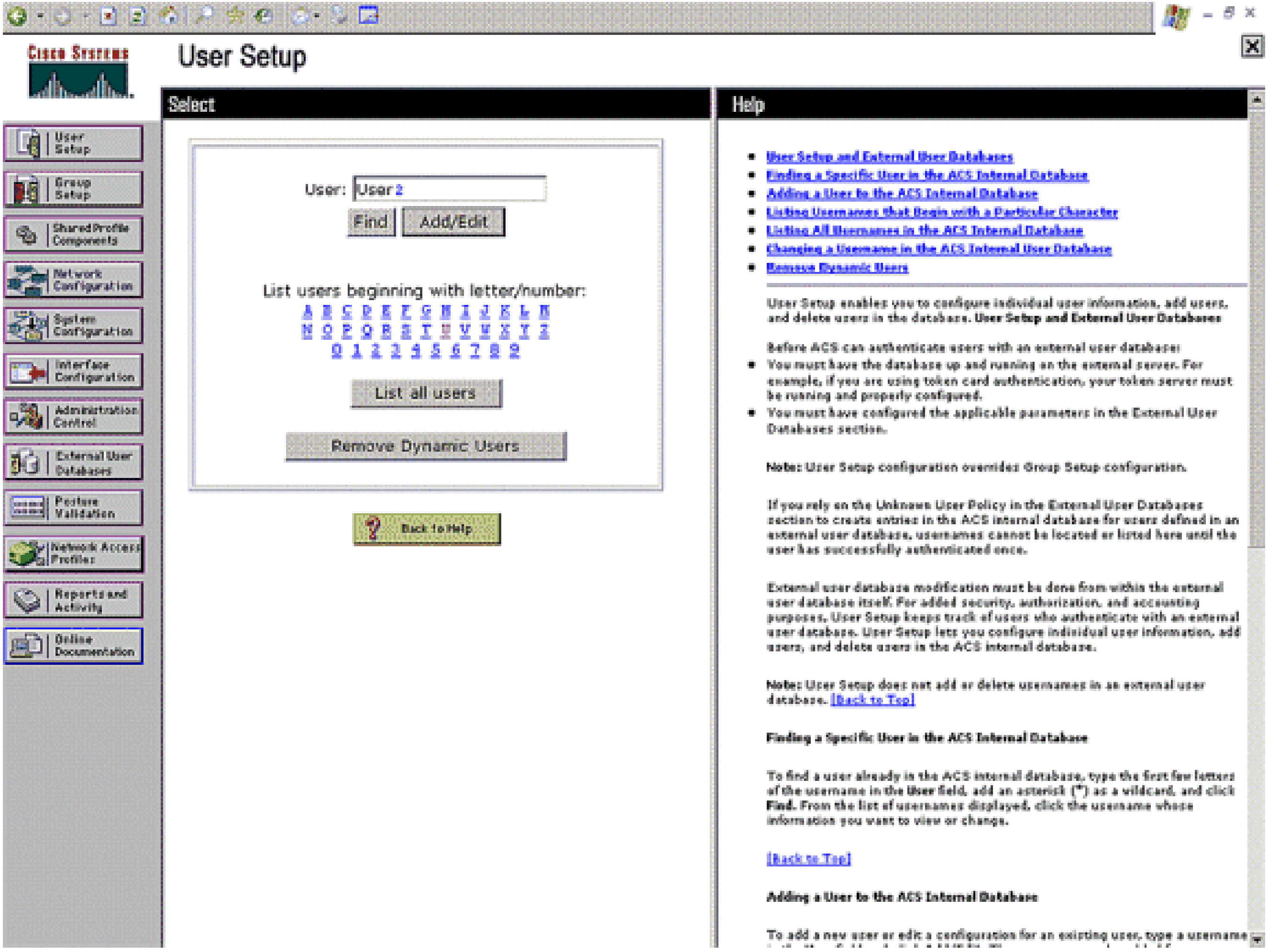
The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click **Delete.** When asked to confirm your action, click **OK.**

[Back to Top]

**Supplementary User Info**

Type the applicable information in any supplemental user information boxes that appear. To add or change fields, click **Interface**

3. 重复相同的步骤创建User2，如下所示。



**Select**

User: User2

List users beginning with letter/number:
A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9

**Help**

- User Setup and External User Databases
- Finding a Specific User in the ACS Internal Database
- Adding a User to the ACS Internal Database
- Listing Usernames that Begin with a Particular Character
- Listing All Usernames in the ACS Internal Database
- Changing a Username in the ACS Internal User Database
- Remove Dynamic Users

User Setup enables you to configure individual user information, add users, and delete users in the database. **User Setup and External User Databases**

Before ACS can authenticate users with an external user database:

- You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
- You must have configured the applicable parameters in the External User Databases section.

**Note:** User Setup configuration overrides Group Setup configuration.

If you rely on the Unknown User Policy in the External User Databases section to create entries in the ACS internal database for users defined in an external user database, usernames cannot be located or listed here until the user has successfully authenticated once.

External user database modification must be done from within the external user database itself. For added security, authorization, and accounting purposes, User Setup keeps track of users who authenticate with an external user database. User Setup lets you configure individual user information, add users, and delete users in the ACS internal database.

**Note:** User Setup does not add or delete usernames in an external user database. [Back to Top]

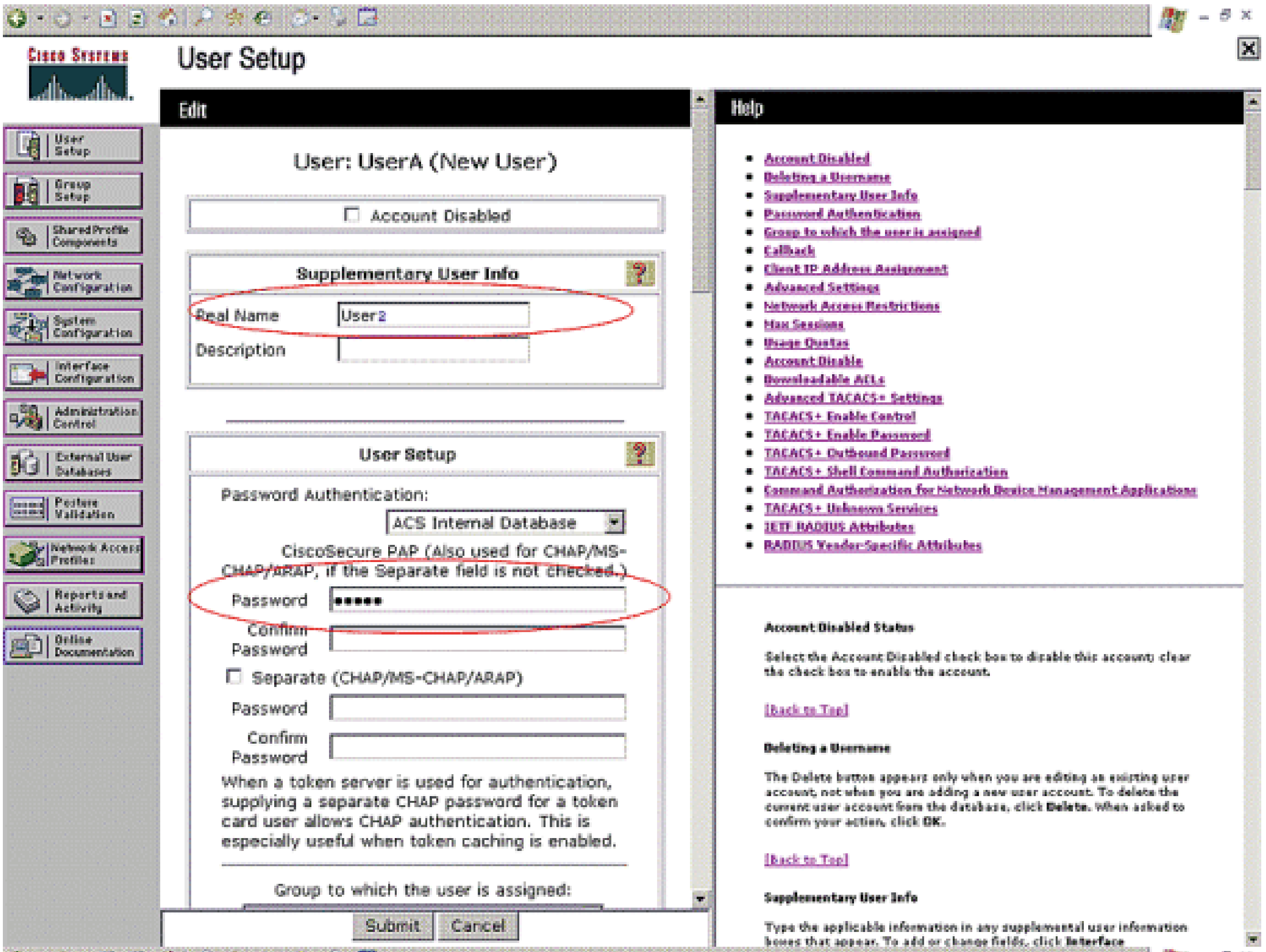
**Finding a Specific User in the ACS Internal Database**

To find a user already in the ACS internal database, type the first few letters of the username in the **User** field, add an asterisk (*) as a wildcard, and click **Find.** From the list of usernames displayed, click the username whose information you want to view or change.

[Back to Top]

**Adding a User to the ACS Internal Database**

To add a new user or edit a configuration for an existing user, type a username



User Setup

Edit

User: UserA (New User)

□ Account Disabled

Supplementary User Info

Real Name: User2

Description:

User Setup

Password Authentication: ACS Internal Database

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 separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

**Account Disabled Status**

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top]

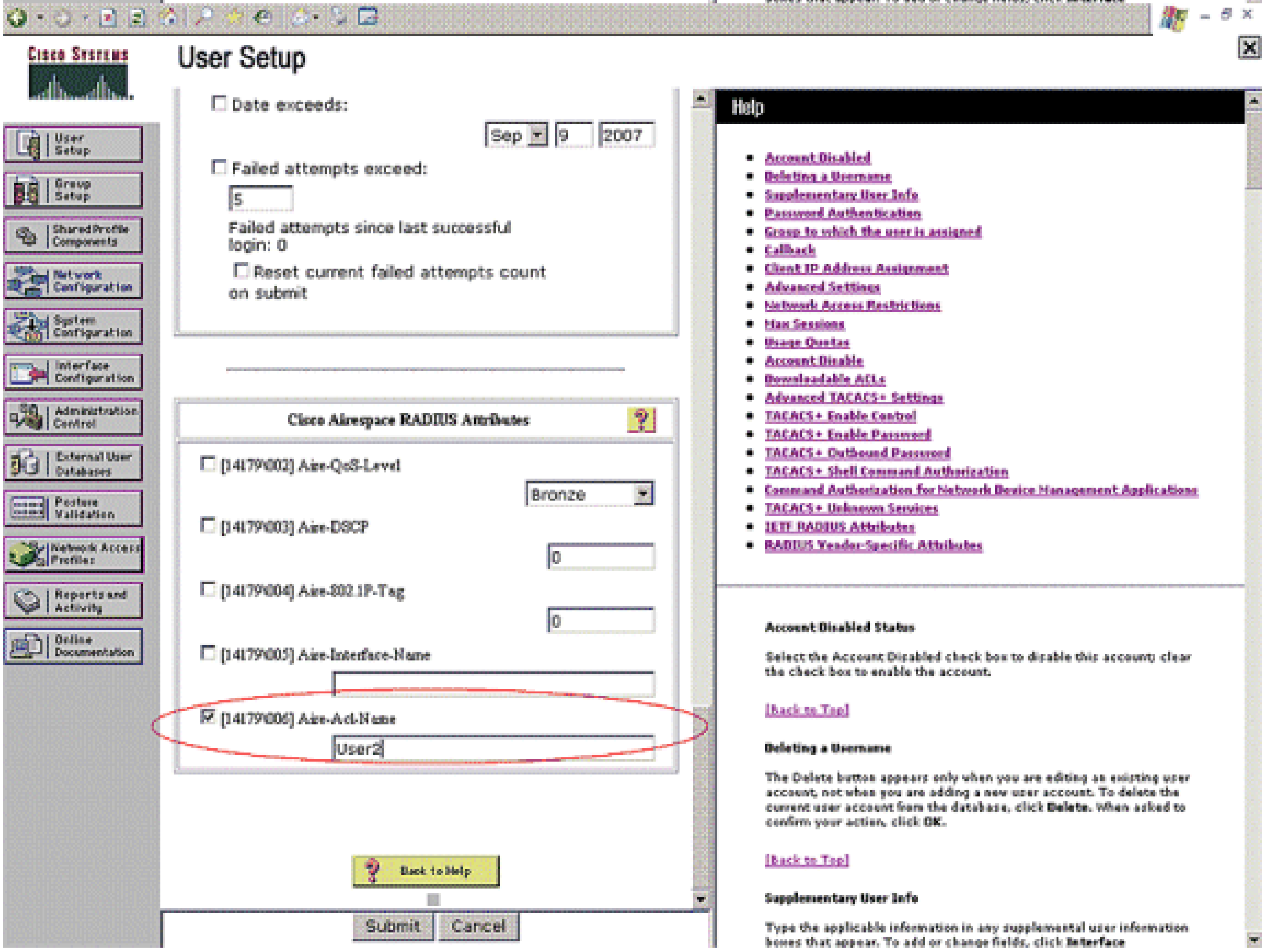
**Deleting a Username**

The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click **Delete**. When asked to confirm your action, click **OK**.

[Back to Top]

**Supplementary User Info**

Type the applicable information in any supplemental user information boxes that appear. To add or change fields, click **Interface**



User Setup

□ Date exceeds: Sep 9 2007

□ Failed attempts exceed: 5

Failed attempts since last successful login: 0

□ Reset current failed attempts count on submit

Cisco Airespace RADIUS Attributes

□ [14179\002] Aire-QoS-Level: Bronze

□ [14179\003] Aire-DSCP: 0

□ [14179\004] Aire-802.1P-Tag: 0

□ [14179\005] Aire-Interface-Name:

☑ [14179\006] Aire-Acl-Name: User2

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

**Account Disabled Status**

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top]

**Deleting a Username**

The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click **Delete**. When asked to confirm your action, click **OK**.

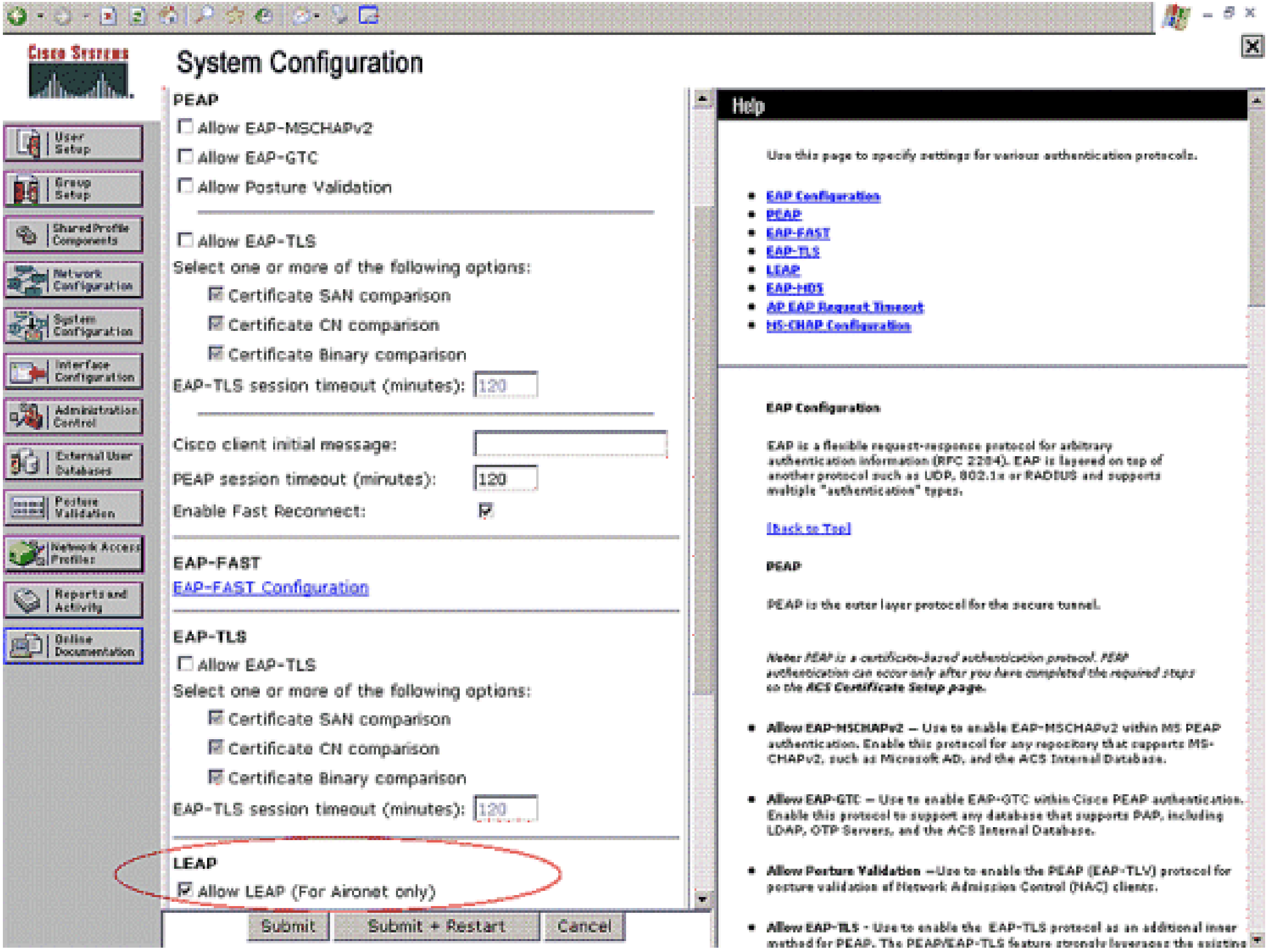
[Back to Top]

**Supplementary User Info**

Type the applicable information in any supplemental user information boxes that appear. To add or change fields, click **Interface**

4. 单击 System Configuration 和 Global Authentication Setup 以确保将身份验证服务器配置为执

**行期望的 EAP 身份验证方法。**在 EAP 配置设置下，选择相应的 EAP 方法。本例使用 LEAP 身份验证。完成后，单击 **Submit。**



System Configuration

PEAP

☐ Allow EAP-MSCHAPv2

☐ Allow EAP-GTC

☐ Allow Posture Validation

☐ Allow EAP-TLS

Select one or more of the following options:

☑ Certificate SAN comparison

☑ Certificate CN comparison

☑ Certificate Binary comparison

EAP-TLS session timeout (minutes): 120

Cisco client initial message:

PEAP session timeout (minutes): 120

Enable Fast Reconnect: ☑

EAP-FAST

EAP-FAST Configuration

EAP-TLS

☐ Allow EAP-TLS

Select one or more of the following options:

☑ Certificate SAN comparison

☑ Certificate CN comparison

☑ Certificate Binary comparison

EAP-TLS session timeout (minutes): 120

LEAP

☑ Allow LEAP (For Aironet only)

Help

Use this page to specify settings for various authentication protocols.

- EAP Configuration
- PEAP
- EAP-FAST
- EAP-TLS
- LEAP
- EAP-MD5
- AP EAP Request Timeout
- MS-CHAP Configuration

EAP Configuration

EAP is a flexible request-response protocol for arbitrary authentication information (RFC 2284). EAP is layered on top of another protocol such as UDP, 802.1x or RADIUS and supports multiple "authentication" types.

[Back to Top]

PEAP

PEAP is the outer layer protocol for the secure tunnel.

*Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have completed the required steps on the* ***ACS Certificate Setup page.***

- **Allow EAP-MSCHAPv2** — Use to enable EAP-MSCHAPv2 within MS PEAP authentication. Enable this protocol for any repository that supports MS-CHAPv2, such as Microsoft AD, and the ACS Internal Database.
- **Allow EAP-GTC** — Use to enable EAP-GTC within Cisco PEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database.
- **Allow Posture Validation** —Use to enable the PEAP (EAP-TLV) protocol for posture validation of Network Admission Control (NAC) clients.
- **Allow EAP-TLS** - Use to enable the EAP-TLS protocol as an additional inner method for PEAP. The PEAP/EAP-TLS feature strongly leverages the existing

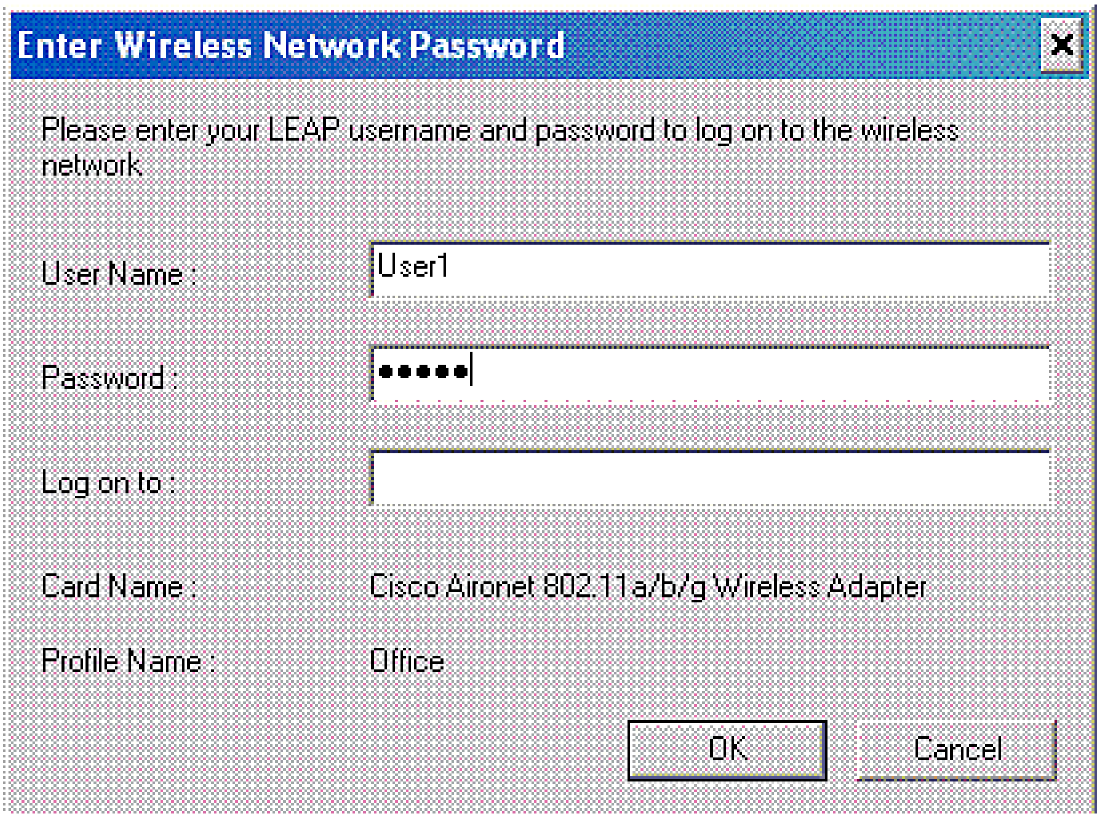
# 验证

使用本部分可确认配置能否正常运行。

尝试将无线客户端与轻量AP与LEAP身份验证关联，以验证配置是否按预期工作。

**注意：本**文档假设客户端配置文件已配置为LEAP身份验证。有关如何为 LEAP 身份验证配置 802.11 a/b/g 无线客户端适配器的详细信息，请参阅使用 EAP 身份验证。

激活无线客户端的配置文件后，即要求用户提供 LEAP 身份验证的用户名/密码。这是当User1尝试向LAP进行身份验证时发生的情况。



Enter Wireless Network Password

Please enter your LEAP username and password to log on to the wireless network

User Name : User1

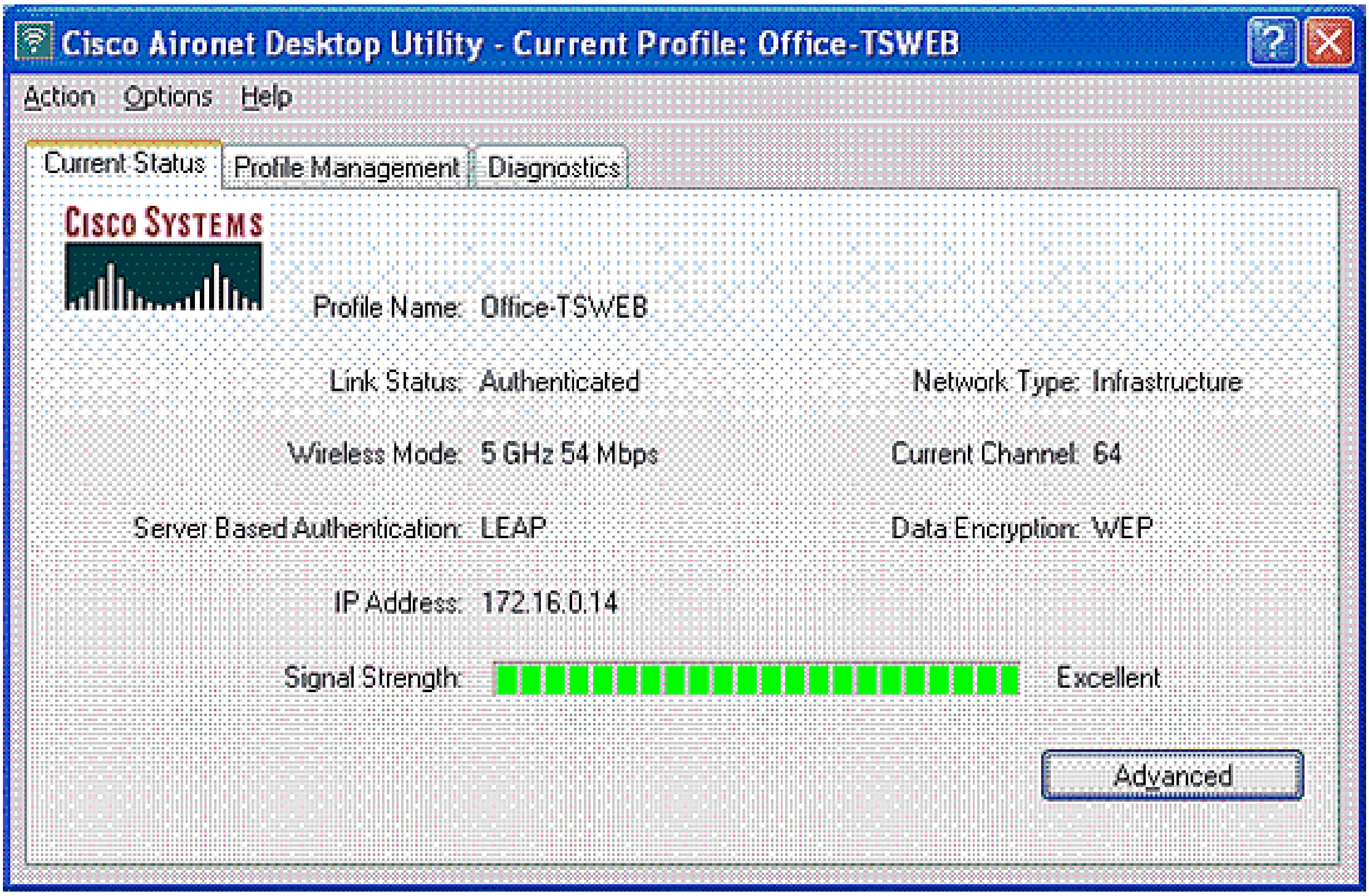
Password : ●●●●●

Log on to :

Card Name : Cisco Aironet 802.11a/b/g Wireless Adapter

Profile Name : Office

轻量 AP 和 WLC 先后将用户凭据传递给外部 RADIUS 服务器（Cisco 安全 ACS）以验证凭据。RADIUS服务器将数据与用户数据库进行比较，并在身份验证成功后将为用户配置的ACL名称返回到WLC。在这种情况下，ACL User1会返回到WLC。



Cisco Aironet Desktop Utility - Current Profile: Office-TSWEB

Profile Name: Office-TSWEB

Link Status: Authenticated

Network Type: Infrastructure

Wireless Mode: 5 GHz 54 Mbps

Current Channel: 64

Server Based Authentication: LEAP

Data Encryption: WEP

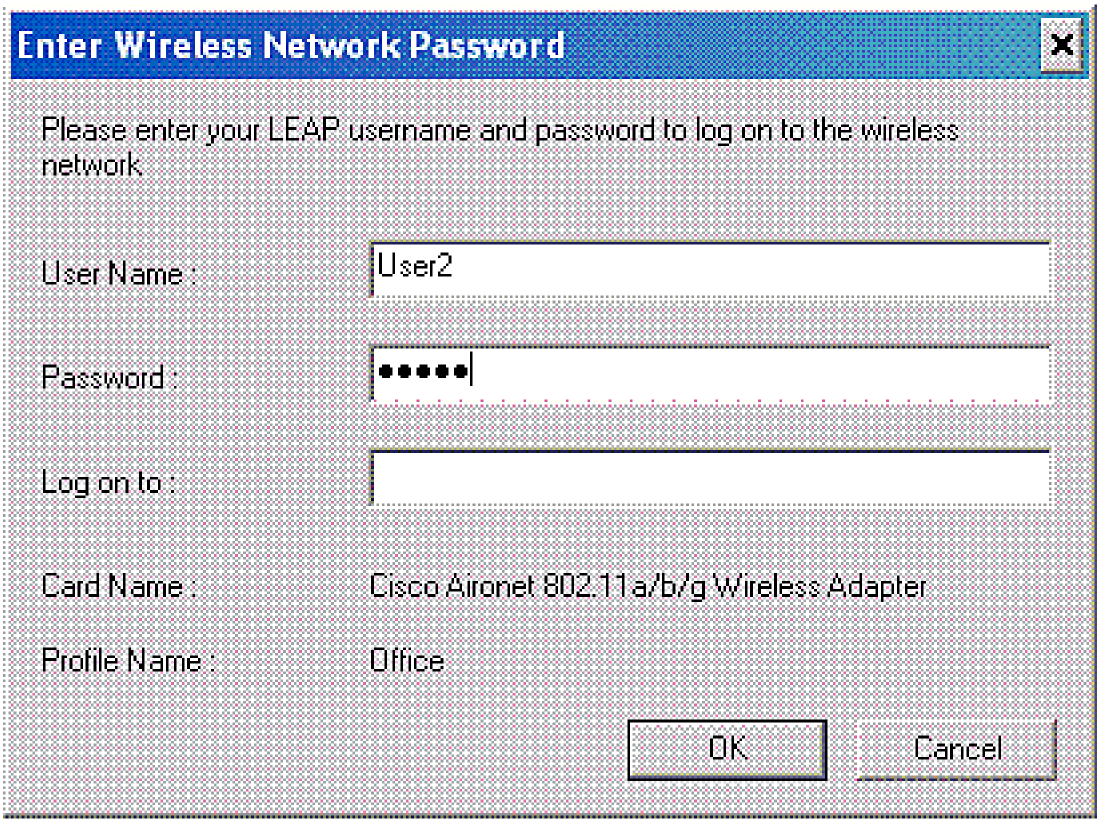
IP Address: 172.16.0.14

Signal Strength: Excellent

无线LAN控制器将此ACL应用于User1。此ping输出显示，User1只能访问服务器172.16.1.100，但不能访问任何其他设备。

```
D:\Documents and Settings\Administrator>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:

Reply from 172.16.1.100: bytes=32 time=3ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255

Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms

D:\Documents and Settings\Administrator>ping 172.16.1.50

Pinging 172.16.1.50 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.50:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

同样，当User2尝试访问WLAN时，RADIUS服务器在身份验证成功后将ACL User2返回到WLC。



Enter Wireless Network Password

Please enter your LEAP username and password to log on to the wireless network

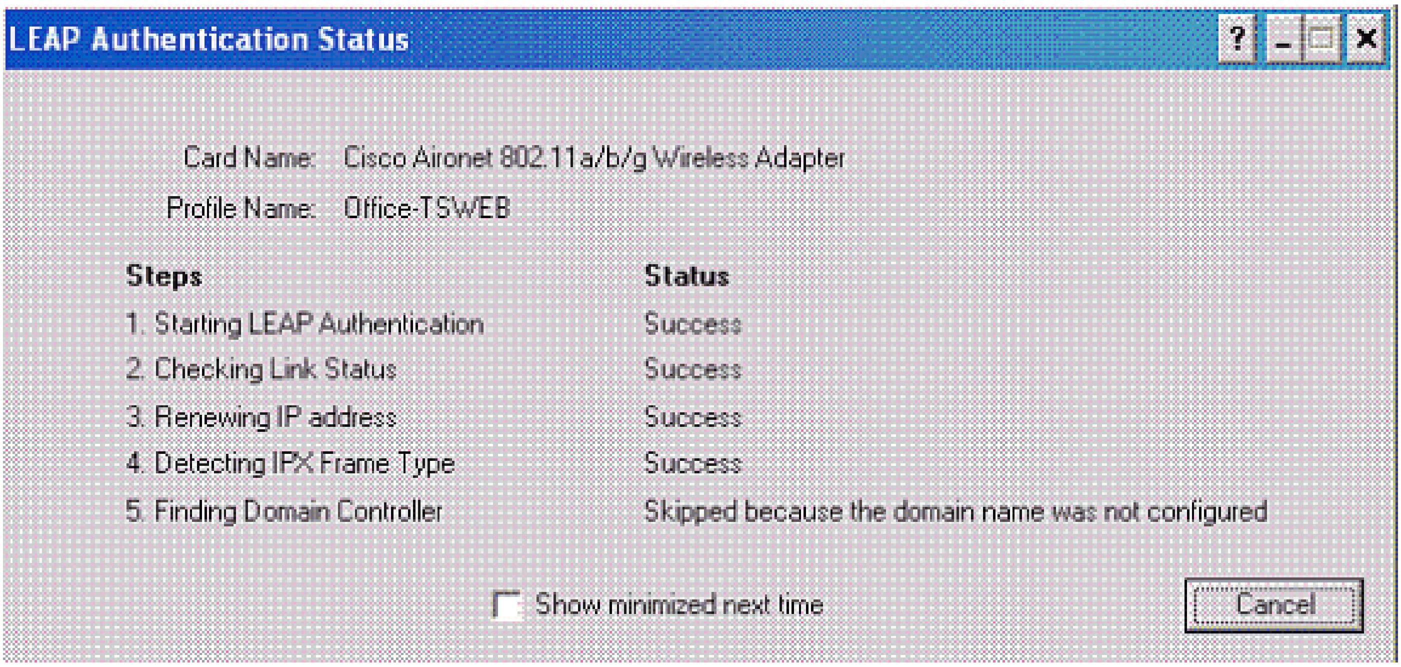
User Name : User2

Password : ●●●●●

Log on to :

Card Name : Cisco Aironet 802.11a/b/g Wireless Adapter

Profile Name : Office



Card Name: Cisco Aironet 802.11a/b/g Wireless Adapter

Profile Name: Office-TSWEB

| Steps | Status |
|---|---|
| 1. Starting LEAP Authentication | Success |
| 2. Checking Link Status | Success |
| 3. Renewing IP address | Success |
| 4. Detecting IPX Frame Type | Success |
| 5. Finding Domain Controller | Skipped because the domain name was not configured |

□ Show minimized next time

无线LAN控制器将此ACL应用于User2。此ping输出显示User2只能访问服务器172.16.1.50，但不能访问任何其他设备。

```
D:\Documents and Settings\Administrator>ping 172.16.1.50

Pinging 172.16.1.50 with 32 bytes of data:

Reply from 172.16.1.50: bytes=32 time=3ms TTL=255
Reply from 172.16.1.50: bytes=32 time=18ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255

Ping statistics for 172.16.1.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 18ms, Average = 5ms

D:\Documents and Settings\Administrator>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

# 故障排除

本部分提供的信息可用于对配置进行故障排除。

在无线LAN控制器上，您还可以使用这些debug命令排除AAA身份验证故障

- **debug aaa all enable** — 配置所有AAA消息的调试

- **debug dot1x packet enable** — 启用所有dot1x数据包的调试
- **debug client <MAC Address>** — 启用无线客户端调试

以下是debug aaa all enable命**令的示**例

**注意：**由于空间限制，输出中的某些行已移至第二行。

```
Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104
Thu Aug 16 14:42:54 2007:       Callback................0x85ed228
Thu Aug 16 14:42:54 2007:       protocolType............0x00140001
Thu Aug 16 14:42:54 2007:       proxyState..............00:40:96:AF:3E:93-03:01
Thu Aug 16 14:42:54 2007:       Packet contains 16 AVPs (not shown)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Successful transmission of Authentication Packet
   (id 1) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00
Thu Aug 16 14:42:54 2007: 00000000: 01 01 00 d0 2d 34 f5 99  b4 19 27 28 eb 5f 35 9c
   ....-4....'(._5.
Thu Aug 16 14:42:54 2007: 00000010: 8f a9 00 dd 01 07 75 73  65 72 31 1f 13 30 30 2d
   ......user1..00-
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46  2d 33 45 2d 39 33 1e 20
   40-96-AF-3E-93..
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35  2d 35 42 2d 46 42 2d 44
   00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65  2d 54 53 57 45 42 05 06
   0:Office-TSWEB..
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d  f4 d2 20 05 77 6c 63 1a
   .......M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00  00 00 01 06 06 00 00 00
   ...7c...........
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d  06 00 00 00 13 40 06 00
   .......=.....@..
Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00  06 51 04 32 30 4f 27 02
   ...A.....Q.20O'.
Thu Aug 16 14:42:54 2007: 00000090: 01 00 25 11 01 00 18 1d  87 9d 0b f9 dd e5 39 0d
   ..%..........9.
Thu Aug 16 14:42:54 2007: 000000a0: 2e 82 eb 17 c6 23 b7 96  dc c3 55 ff 7c 51 4e 75
   .....#....U.|QNu
Thu Aug 16 14:42:54 2007: 000000b0: 73 65 72 31 18 0a 53 56  43 3d 30 2e 31 3b 50 12
   ser1..SVC=0.1;P.
Thu Aug 16 14:42:54 2007: 000000c0: 1a d5 3b 35 5e 93 11 c0  c6 2f 5e f5 65 e9 3e 2d
   ..;5^..../^.e.>-
Thu Aug 16 14:42:54 2007: 00000000: 0b 01 00 36 8c 31 6a b4  27 e6 d4 0e 1b 8e 5d 19
   ...6.1j.'.....].
Thu Aug 16 14:42:54 2007: 00000010: 60 1c c2 16 4f 06 03 01  00 04 18 0a 53 56 43 3d
   ...O.......SVC=
Thu Aug 16 14:42:54 2007: 00000020: 30 2e 31 3b 50 12 6c fb  90 ec 48 9b fb d7 ce ca
   0.1;P.l...H.....
Thu Aug 16 14:42:54 2007: 00000030: 3b 64 93 10 fe 09      ;d....
Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=11
Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=11
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Access-Challenge received from RADIUS server
   10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
Thu Aug 16 14:42:54 2007:       structureSize............104
Thu Aug 16 14:42:54 2007:       resultCode...............255
Thu Aug 16 14:42:54 2007:       protocolUsed............0x00000001
Thu Aug 16 14:42:54 2007:       proxyState...............
   00:40:96:AF:3E:93-03:01
Thu Aug 16 14:42:54 2007:       Packet contains 3 AVPs (not shown)
Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104
Thu Aug 16 14:42:54 2007:       Callback................0x85ed228
Thu Aug 16 14:42:54 2007:       protocolType...........0x00140001
Thu Aug 16 14:42:54 2007:       proxyState........................
   00:40:96:AF:3E:93-03:02
Thu Aug 16 14:42:54 2007:       Packet contains 16 AVPs (not shown)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Successful transmission of Authentication Packet (id 2) to 10.77.244.196:1812,
proxy state 00:40:96:af:3e:93-00:00
Thu Aug 16 14:42:54 2007: 00000000: 01 02 00 c0 38 b6 b2 20  ff 5b f2 16 64 df 02 61
   ....8....[..d..a
Thu Aug 16 14:42:54 2007: 00000010: cf f5 93 4b 01 07 75 73  65 72 31 1f 13 30 30 2d
   ...K..User1..00-
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46  2d 33 45 2d 39 33 1e 20
   40-96-AF-3E-93..
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35  2d 35 42 2d 46 42 2d 44
   00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65  2d 54 53 57 45 42 05 06
   0:Office..
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d  f4 d2 20 05 77 6c 63 1a
   .......M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00  00 00 01 06 06 00 00 00
   ...7c...........
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d  06 00 00 00 13 40 06 00
   .......=.....@..
Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00  06 51 04 32 30 4f 17 01
   ...A.....Q.20O..
Thu Aug 16 14:42:54 2007: 00000090: 01 00 15 11 01 00 08 0f  14 05 65 1b 28 61 c9 75
   ..........e.(a.u
Thu Aug 16 14:42:54 2007: 000000a0: 73 65 72 31 18 0a 53 56  43 3d 30 2e 31 3b 50 12
   ser1..SVC=0.1;P.
Thu Aug 16 14:42:54 2007: 000000b0: 05 ba 6b af fe a4 b0 d1  a2 94 f8 39 80 ca 3c 96
   ..k........9..<.
Thu Aug 16 14:42:54 2007: 00000000: 02 02 00 ce c9 3d 5d c8  6c 07 8e fb 58 84 8d f6
   .....=].l...X...
Thu Aug 16 14:42:54 2007: 00000010: 33 6d 93 21 08 06 ff ff  ff ff 4f 27 02 01 00 25
   3m.!......O'...%
Thu Aug 16 14:42:54 2007: 00000020: 11 01 00 18 e5 e5 31 1e  33 b5 4e 69 90 e7 84 25
   ......1.3.Ni...%
Thu Aug 16 14:42:54 2007: 00000030: 42 a9 20 ac 84 33 9f 87  ca dc c9 b3 75 73 65 72
   B....3......user
Thu Aug 16 14:42:54 2007: 00000040: 31 1a 3b 00 00 00 09 01  35 6c 65 61 70 3a 73 65
   1.;.....5leap:se
Thu Aug 16 14:42:54 2007: 00000050: 73 73 69 6f 6e 2d 6b 65  79 3d 29 80 1d 2c 1c 85
   ssion-key=)..,..
Thu Aug 16 14:42:54 2007: 00000060: db 1c 29 7e 40 8a b8 93  69 2a 55 d2 e5 46 89 8b
   ..)~@...i*U..F..
Thu Aug 16 14:42:54 2007: 00000070: 2c 3b 65 49 3e 44 cf 7e  95 29 47 54 1a 1f 00 00
   ,;eI>D.~.)GT....
Thu Aug 16 14:42:54 2007: 00000080: 00 09 01 19 61 75 74 68  2d 61 6c 67 6f 2d 74 79
   ....auth-algo-ty
Thu Aug 16 14:42:54 2007: 00000090: 70 65 3d 65 61 70 2d 6c  65 61 70 1a 0d 00 00 37
   pe=eap-leap....7
Thu Aug 16 14:42:54 2007: 000000a0: 63 06 07 55 73 65 72 31  19 14 43 41 43 53 3a 30
   c..User1..CACS:0
Thu Aug 16 14:42:54 2007: 000000b0: 2f 39 2f 61 34 64 66 34  64 32 2f 31 50 12 9a 71
   /9/a4df4d2/1P..q
Thu Aug 16 14:42:54 2007: 000000c0: 09 99 7d 74 89 ad af e5  c8 b1 71 94 97 d1
   ..}t......q...
Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=2
Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=2
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Access-Accept received from RADIUS server
   10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
Thu Aug 16 14:42:54 2007:       structureSize...........236
Thu Aug 16 14:42:54 2007:       resultCode...............0
Thu Aug 16 14:42:54 2007:       protocolUsed.............0x0
0000001
Thu Aug 16 14:42:54 2007:       proxyState...............00:
40:96:AF:3E:93-03:02
Thu Aug 16 14:42:54 2007:  Packet contains 6 AVPs:
Thu Aug 16 14:42:54 2007:  AVP[01] Framed-IP-Address..........0xffffffff (-1)
   (4 bytes)
Thu Aug 16 14:42:54 2007:  AVP[02] EAP-Message................DATA (37 bytes)
Thu Aug 16 14:42:54 2007:  AVP[03] Cisco / LEAP-Session-Key...DATA (16 bytes)
Thu Aug 16 14:42:54 2007:  AVP[04] Airespace / ACL-Name.......User1 (5 bytes)
Thu Aug 16 14:42:54 2007:  AVP[05] Class......................CACS:0/9/a4df4d2/1
   (18 bytes)
Thu Aug 16 14:42:54 2007:  AVP[06] Message-Authenticator......DATA (16 bytes)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Applying new AAA override
   for station 00:40:96:af:3e:93
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Override values
   for station 00:40:96:af:3e:93
             source: 4, valid bits: 0x400
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                       vlanIfName: '',
aclName:User1
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
   Inserting new RADIUS override into chain for station 00:40:96:af:3e:93
```

您可以结合使用**show wlan summary**命令来识别哪些WLAN使用RADIUS服务器身份验证。然后，您可以查看**show client summary**命令，以查看在RADIUS WLAN上成功验证哪些MAC地址（客户端）。也可以将此与 Cisco 安全 ACS 的 passed attempts 或 failed attempts 日志关联。

Cisco 建议您使用无线客户端测试您的 ACL 配置以确保正确配置。如果ACL无法正常运行，请检验ACL网页上的ACL，并检验您的ACL更改是否已应用到控制器的接口。

您也可使用这些 show 命令验证您的配置：

- **show acl summary — 为了显示在控制器上配置的 ACL，请使用 show acl summary 命令。**

示例如下：

```
(Cisco Controller) >show acl summary

ACL Name                         Applied
-------------------------------- -------
User1                                  Yes
User2                                  Yes
```

- **show acl detailed**<ACL_Name> — 显示有关已配置ACL的详细信息。示例如下：**注意：**由于空间限制，输出中的某些行已移至第二行。

```
Cisco Controller) >show acl detailed User1

                Source                         Destination
   Source Port   Dest Port
I  Dir       IP Address/Netmask              IP Address/Netmask
   Prot     Range         Range     DSCP   Action
-- --- ------------------------------- -------------------------------
   ---- ----------- ----------- ----    ------
```

```
 1  In      172.16.0.0/255.255.0.0        172.16.1.100/255.255.255.255
   Any  0-65535       0-65535   Any    Permit
 2 Out    172.16.1.100/255.255.255.255      172.16.0.0/255.255.0.0
   Any  0-65535       0-65535   Any    Permit


(Cisco Controller) >show acl detailed User2

                   Source                       Destination
   Source Port   Dest Port
I  Dir       IP Address/Netmask              IP Address/Netmask
   Prot     Range        Range     DSCP Action
-- --- ------------------------------- -------------------------------
   ---- ----------- ----------- ---- ------
1  In      172.16.0.0/255.255.0.0         172.16.1.50/255.255.255.255
   Any   0-65535       0-65535     Any  Permit
2 Out     172.16.1.50/255.255.255.255      172.16.0.0/255.255.0.0
   Any   0-65535       0-65535     Any  Permit
```

- **show client detail** <MAC Address of the client> — 显示有关无线客户端的详细信息。

## 故障排除提示

使用以下提示进行故障排除：

- 在控制器上验证RADIUS服务器处于活动状态，而不是处于备用或禁用状态。
- 在控制器上，检查RADIUS服务器是否从WLAN(SSID)的下拉菜单中选择。
- 检查 RADIUS 服务器是否从无线客户端接收并验证身份验证请求。
- 检查 ACS 服务器上的 Passed Authentications 和 Failed Attempts 报告以完成此操作。在ACS服务器上的报表和活动下可获得这些报表。

# 相关信息

- 在无线局域网控制器的ACL ：规则、限制和示例
- 无线 LAN 控制器中的 ACL 配置示例
- 无线 LAN 控制器 (WLC) 的 MAC 过滤器配置示例
- Cisco 无线局域网控制器配置指南 5.2 版
- 技术支持和文档 - Cisco Systems