根据 WLC 和 Cisco Secure ACS 的 SSID 限制 WLAN 访问的配置示例

Contents

Introduction

本文提供基于服务集标识符 (SSID) 限制每用户对 WLAN 的访问权限的配置示例。

Prerequisites

Requirements

尝试进行此配置之前，请确保满足以下要求：

- 了解如何配置无线 LAN 控制器 (WLC) 和轻量接入点 (LAP) 以执行基本的操作
- 如何配置 Cisco 安全访问控制服务器 (ACS) 的基本知识
- 轻量级接入点协议(LWAPP)和无线安全方法知识

Components Used

本文档中的信息基于以下软件和硬件版本：

- 运行固件 4.0 的 Cisco 2000 系列 WLC
- Cisco 1000系列LAP
- Cisco Secure ACS 服务器版本 3.2

- 运行固件版本 2.6 的 Cisco 802.11a/b/g 无线客户端适配器
- Cisco Aironet Desktop Utility (ADU) 版本 2.6

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

背景信息

使用基于 SSID 的 WLAN 访问，用户可以基于他们使用的 SSID 进行认证，从而连接到 WLAN。Cisco Secure ACS 服务器用于认证用户。Cisco Secure ACS 上的认证分为两个阶段：

1. EAP验证
2. Cisco Secure ACS 上基于网络访问限制 (NAR) 的 SSID 认证

如果 EAP 和基于 SSID 的认证成功，则用户可以访问 WLAN，否则将取消用户关联。

Cisco Secure ACS 使用 NAR 功能基于 SSID 限制用户访问。NAR 是您在 Cisco Secure ACS 中设定的定义，规定了用户在访问网络之前必须满足的额外条件。Cisco Secure ACS 使用从您的 AAA 客户端发送的属性的信息来满足这些条件。尽管有多种设置 NAR 的方法，但这些方法都基于匹配 AAA 客户端发送的属性信息。所以，若要使用有效的 NAR，您必须了解 AAA 客户端发送的属性的格式和内容。

设置 NAR 时，可以选择过滤器是积极运行还是消极运行。即根据比较 AAA 客户端发送的信息和 NAR 存储的信息，在 NAR 中指定是允许还是拒绝网络访问。不过，如果 NAR 没有充足的信息以运行，将会默认为拒绝访问。

可以针对某个特定用户或用户组定义一个 NAR，然后将其应用到该用户或用户组。有关详细信息，请参阅网络访问限制白皮书。

Cisco Secure ACS 支持两种类型的 NAR 过滤器：

1. **基于 IP 的过滤器** — 基于 IP 的 NAR 过滤器根据最终用户客户端和 AAA 客户端的 IP 地址限制访问。有关此种过滤器的详细信息，请参阅关于基于 IP 的 NAR 过滤器。
2. **非基于 IP 的过滤器** — 非基于 IP 的 NAR 过滤器根据从 AAA 客户端发送的值的简单字符串比较限制访问。其发送的值可以是主叫线路 ID (CLI) 号、Dialed Number Identification Service (DNIS) 号、MAC 地址或者来自客户端的其他值。为了使此种 NAR 运行，NAR 说明中的值必须与客户端发送的值完全匹配，包括其使用的任何格式。例如，(217) 555-4534 不匹配 217-555-4534。有关此种过滤器的详细信息，请参阅关于非基于 IP 的 NAR 过滤器。

本文档使用非基于 IP 的过滤器执行基于 SSID 的认证。非基于 IP 的 NAR 过滤器（即基于 DNIS/CLI 的 NAR 过滤器）是一个允许或拒绝呼叫/接入点位置列表，在未建立基于 IP 的连接时，可以使用该过滤器进行 AAA 客户端限制。非基于 IP 的 NAR 功能通常使用 CLI 编号和 DNIS 编号。在使用 DNIS/CLI 字段时，存在一些例外情况。您可以在 DNIS 字段中输入 SSID 名称并执行基于 SSID 的认证。这是因为 WLC 将 DNIS 属性、SSID 名称发送到 RADIUS 服务器。因此，如果在用户或用户组中构建 DNIS NAR，您能创建每用户 SSID 限制。

如果使用 RADIUS，此处列出的 NAR 字段使用这些值：

- **AAA client** — 使用 NAS-IP-address（属性 4）或（如果 NAS-IP-address 不存在）NAS-identifier（RADIUS 属性 32）。
- **端口** — 使用 NAS-port（属性 5）或（如果 NAS-port 不存在）NAS-port-ID（属性 87）。
- **CLI** —使用呼叫位置ID (属性31)。
- **DNIS** —使用呼叫位置ID (属性30)。

有关 NAR 使用的详细信息，请参阅网络访问限制。

因为 WLC 发送 DNIS 属性和 SSID 名称，您可以创建每用户 SSID 限制。对于 WLC，NAR 字段有这些值：

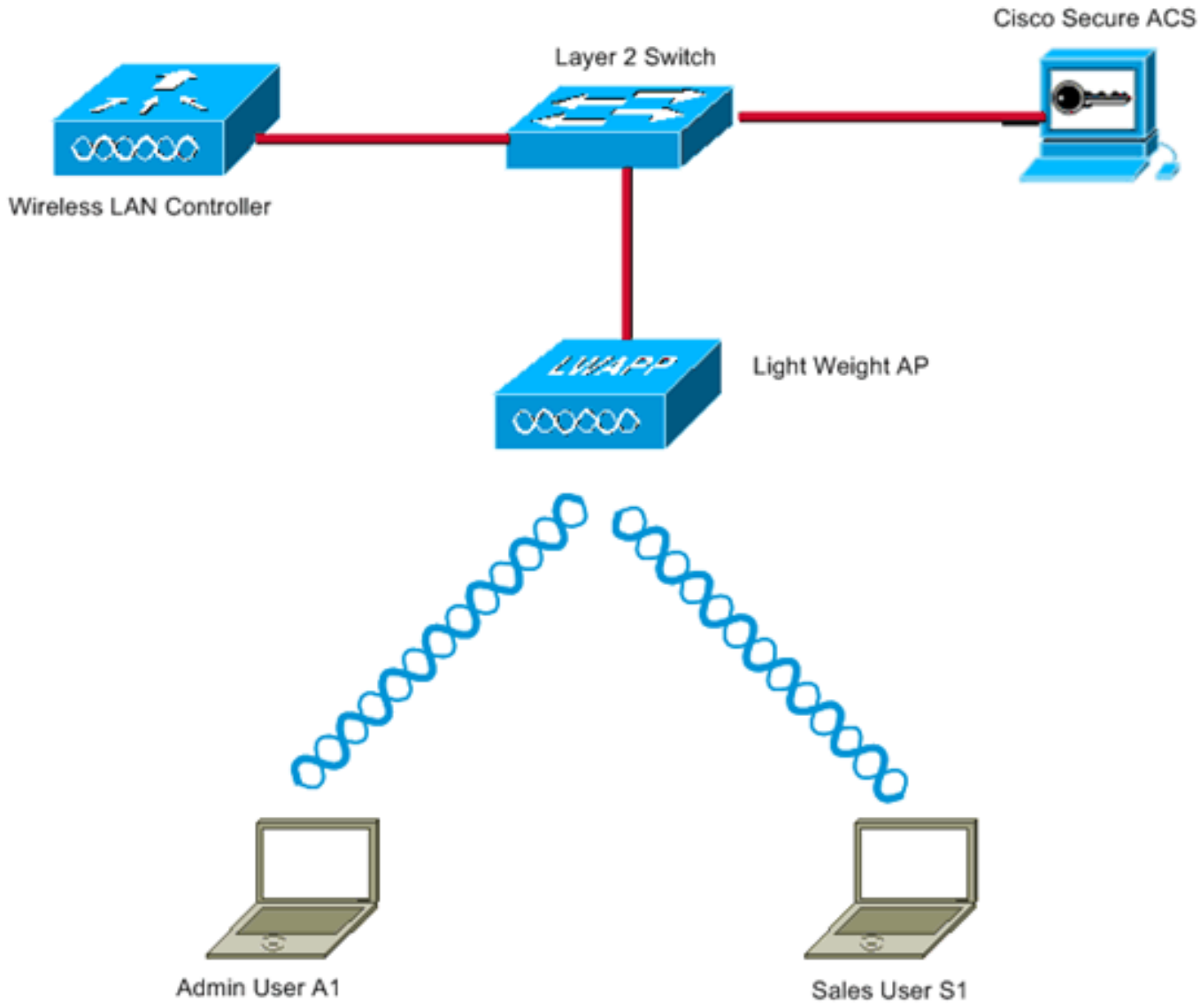
- **AAA client** — WLC IP 地址
- **端口**— *
- **CLI** — *
- **DNIS** — *ssidname

本文档的其余部分将提供实现此目的的示例。

网络设置

在此示例设置中，WLC 在 LAP 中注册。使用了两个 WLAN。一个 WLAN 用于管理部门用户，另一个 WLAN 用于销售部门用户。无线客户端 A1（管理员用户）和 S1（销售用户）连接到无线网络。您需要配置 WLC 和 RADIUS 服务器使管理员用户 A1 仅能访问 WLAN **Admin** 并且对 WLAN **Sales** 访问受限，而销售用户 S1 可以访问 WLAN **Sales** 并且对 WLAN **Admin** 访问受限。所有用户将 LEAP 认证作为第 2 层认证方法。

Note: 本文档假设 WLC 已在控制器中注册。如果您对 WLC 不熟悉，并且不会配置 WLC 进行基本操作，请参阅 轻量 AP (LAP) 注册到无线 LAN 控制器 (WLC)。



WLC Management Interface IP address : 172.16.1.30/16
WLC AP-Manager Interface IP address: 172.16.1.31/16
Cisco Secure ACS server IP address: 172.16.1.60/16

SSID for the Admin department users : Admin
SSID for Sales department users: Sales

Configure

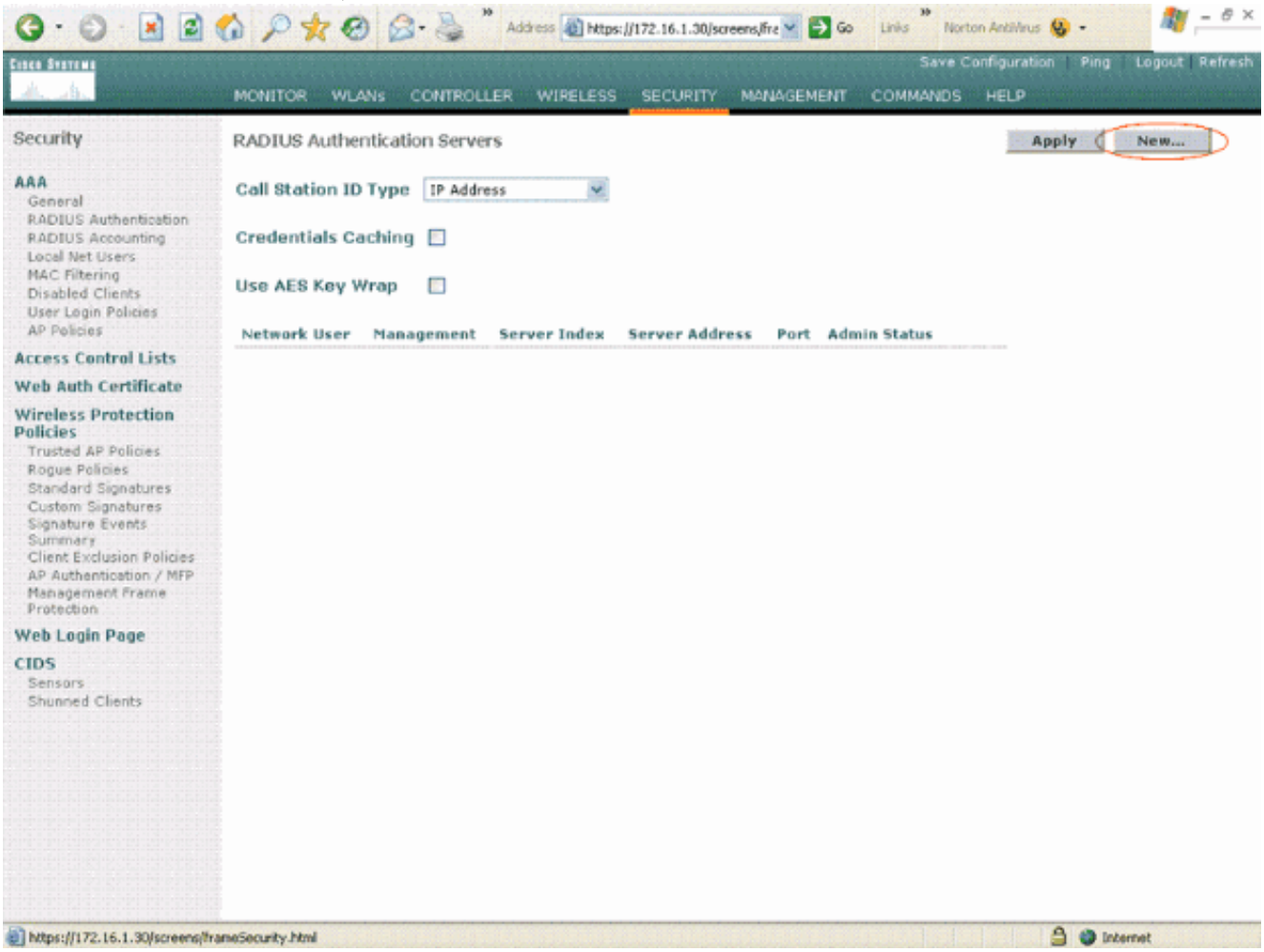
为了针对此设置配置设备，您需要：

1. 需要为 WLC 配置两个 WLAN 和 RADIUS 服务器。
2. 配置 Cisco Secure ACS。
3. 配置无线客户端并验证。

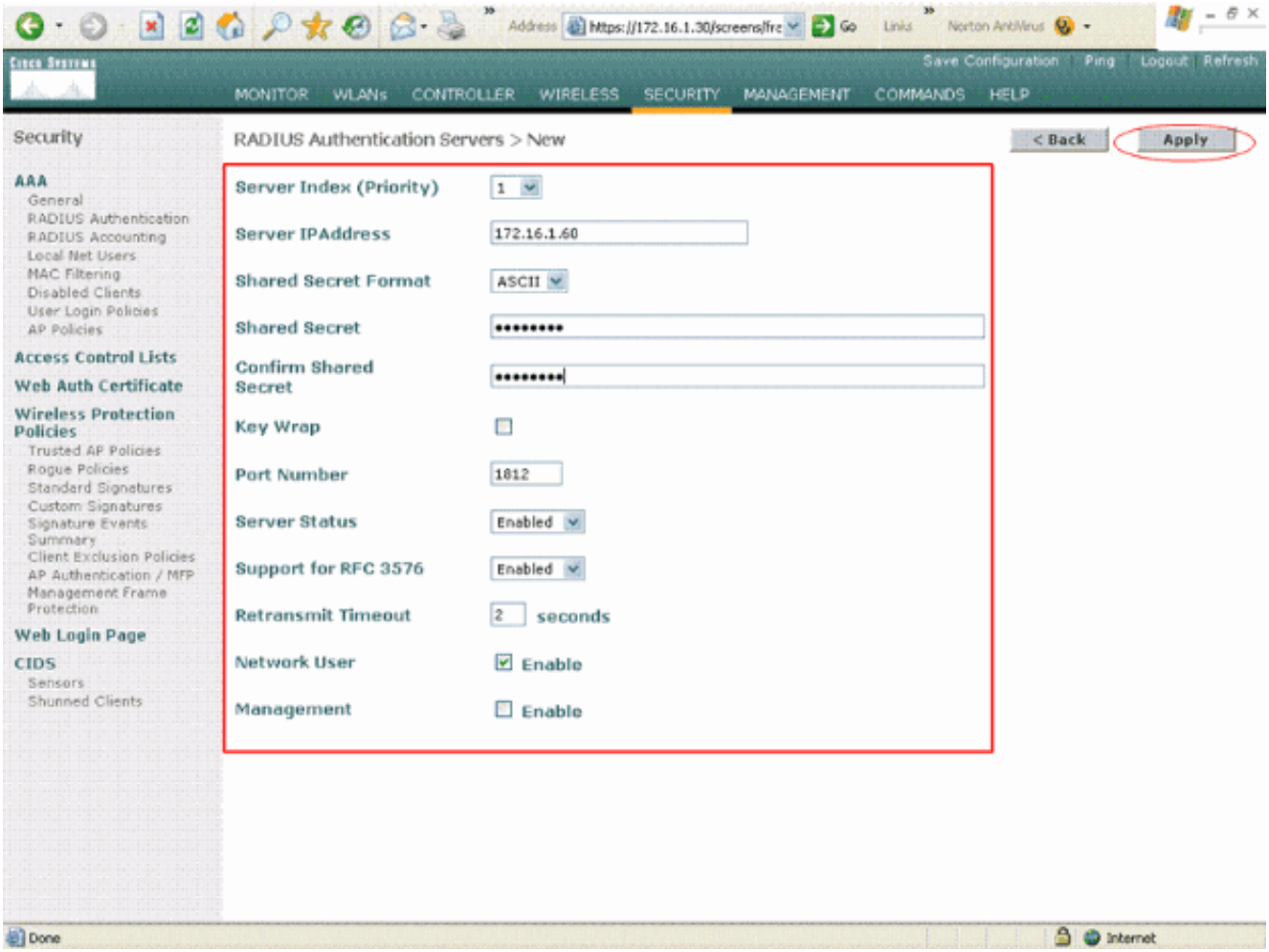
配置 WLC

要配置 WLC 使用该设置，请完成以下步骤：

1. 需要配置 WLC 以转发用户凭证到外部 RADIUS 服务器。外部 RADIUS 服务器（在这种情况下是 Cisco Secure ACS）然后验证用户凭证并提供对无线客户端的访问权限。完成这些步骤：从控制器的 GUI 中选择 **Security > RADIUS Authentication** ，以便显示 RADIUS Authentication Servers 页。

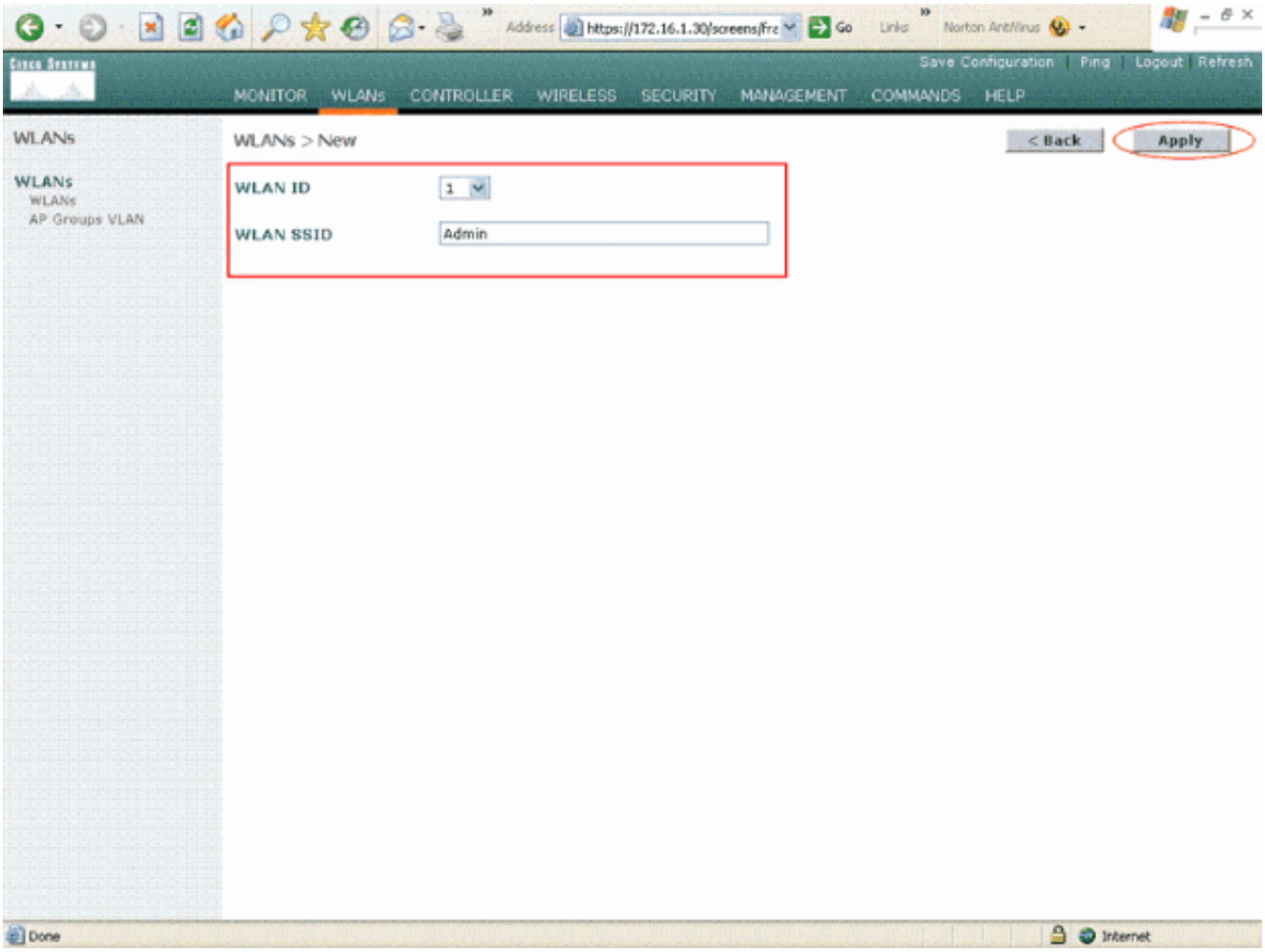


单击 **New** 以定义 RADIUS 服务器参数。这些参数包括RADIUS服务器IP地址、共有的秘密、端口号和服务器状态。“网络用户”和“管理”复选框决定基于 RADIUS 的身份验证是否适用于管理和网络用户。本例使用 Cisco 安全 ACS 作为 RADIUS 服务器，其 IP 地址为 172.16.1.60。

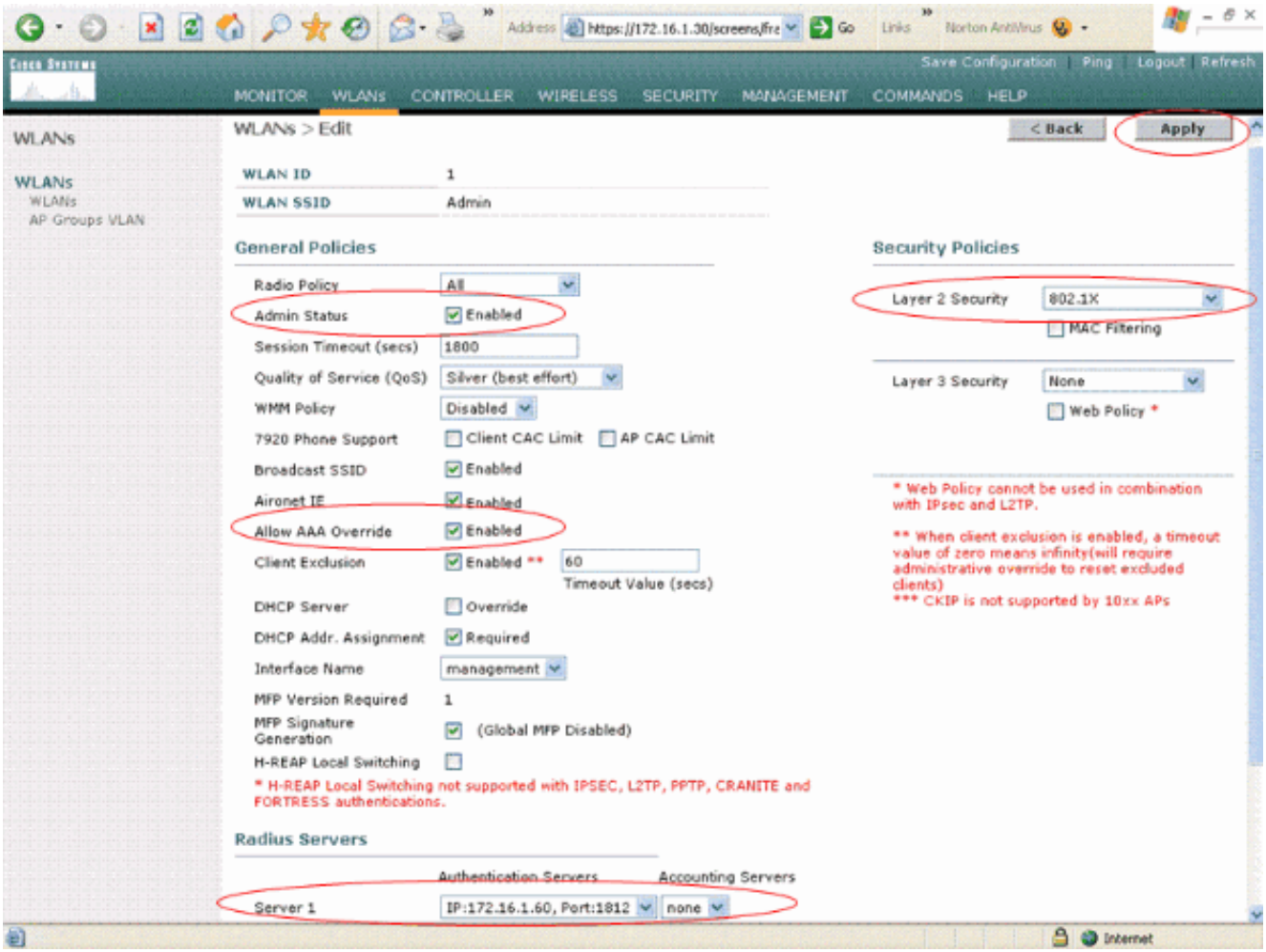


单击 **Apply**。

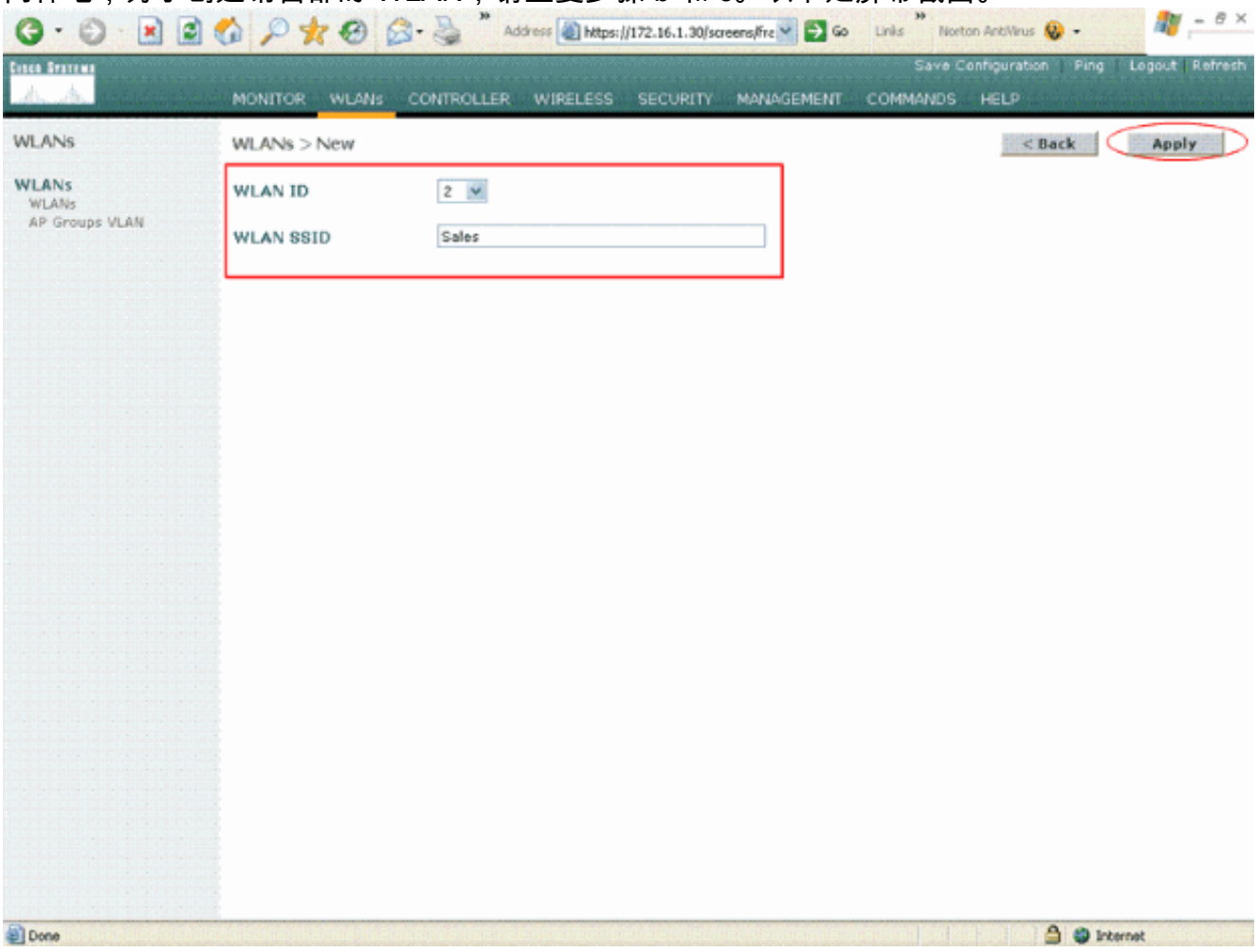
2. 为管理部门配置参数为 SSID **Admin** 的 WLAN，为销售部门配置参数为 SSID **Sales** 的 WLAN。要执行上述操作，请完成以下步骤：要创建 WLAN，请从控制器 GUI 中单击 **WLANs**。随即显示 WLAN 窗口。该窗口列出了控制器中配置的 WLAN。要配置新的 WLAN，请单击 **New**。此示例为管理部门创建了名为 **Admin** 的 WLAN，并且 WLAN ID 是 **1.** 单击 **Apply**。

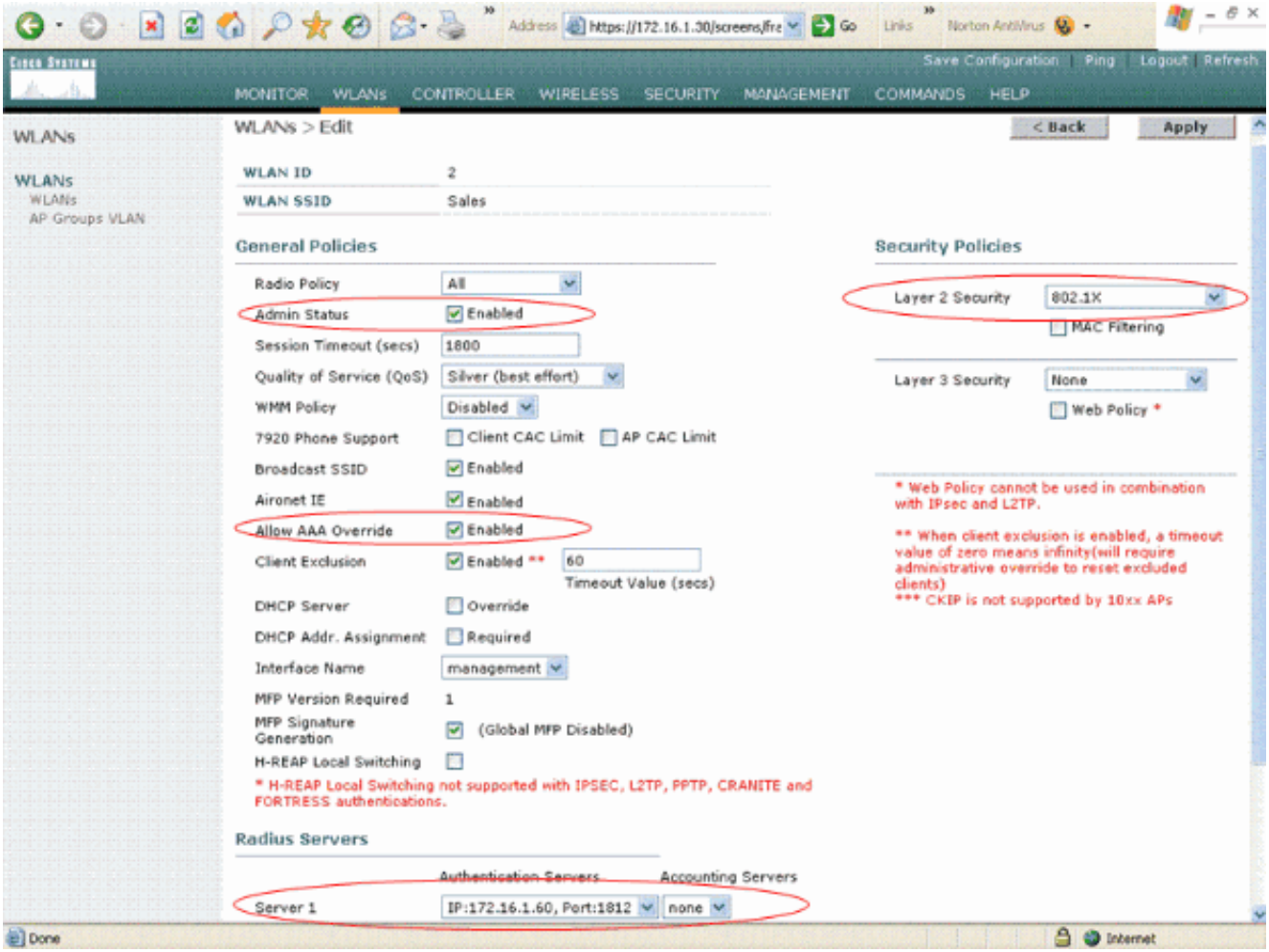


在 **WLAN > Edit 窗口**中，定义特定于该 WLAN 的参数：从 Layer 2 Security 下拉菜单中选择 **802.1x**。默认情况下，Layer 2 Security 选项为 802.1x。这将为该 WLAN 启用 802.1x/EAP 认证。在一般策略下，选中 **AAA override** 框。如果“AAA 覆盖”处于启用状态，并且客户端拥有冲突的 AAA 和控制器 WLAN 认证参数，则由 AAA 服务器执行客户端认证。从 RADIUS Servers 下的下拉菜单中选择相应的 RADIUS 服务器。可以修改其他参数根据WLAN网络的需求。单击 **Apply**。



同样地，为了创建销售部的 WLAN，请重复步骤 b 和 c。以下是屏幕截图。





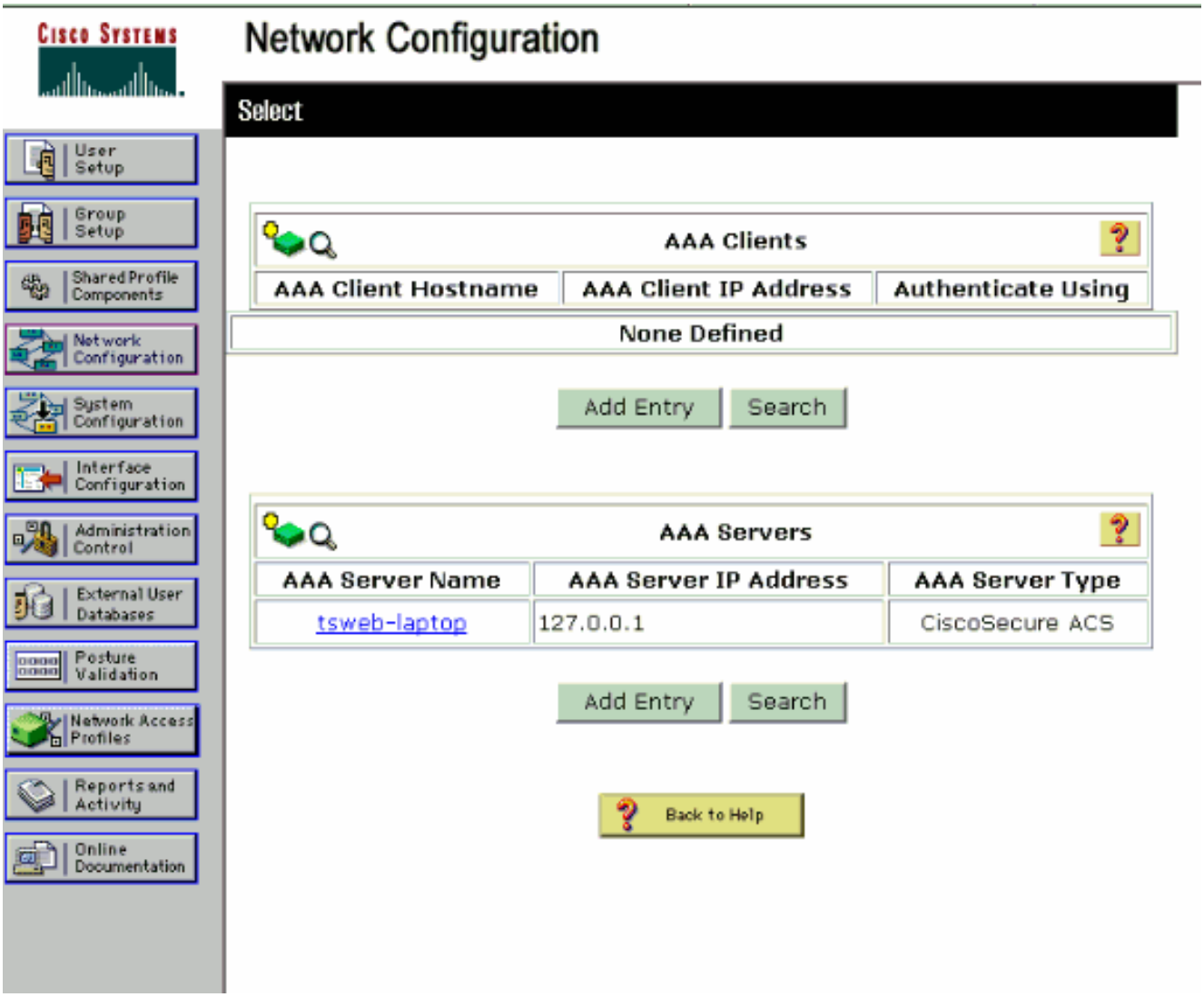
配置 Cisco Secure ACS

在 Cisco Secure ACS 服务器上，您需要：

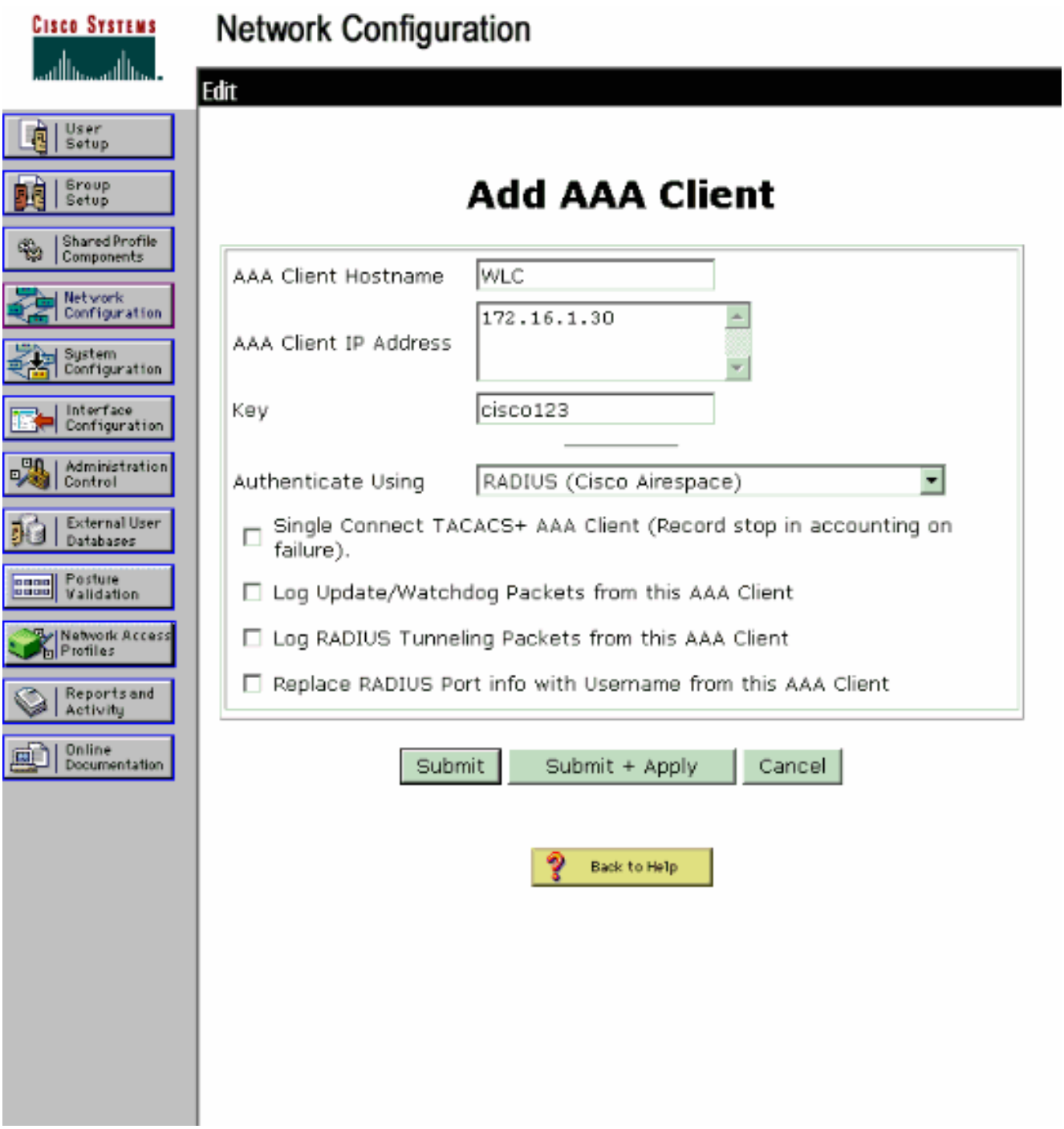
1. 配置 WLC 作为 AAA 客户端。
2. 创建用户数据库并定义基于 SSID 的认证的 NAR。
3. 启用 EAP 认证。

在 Cisco Secure ACS 上完成以下步骤：

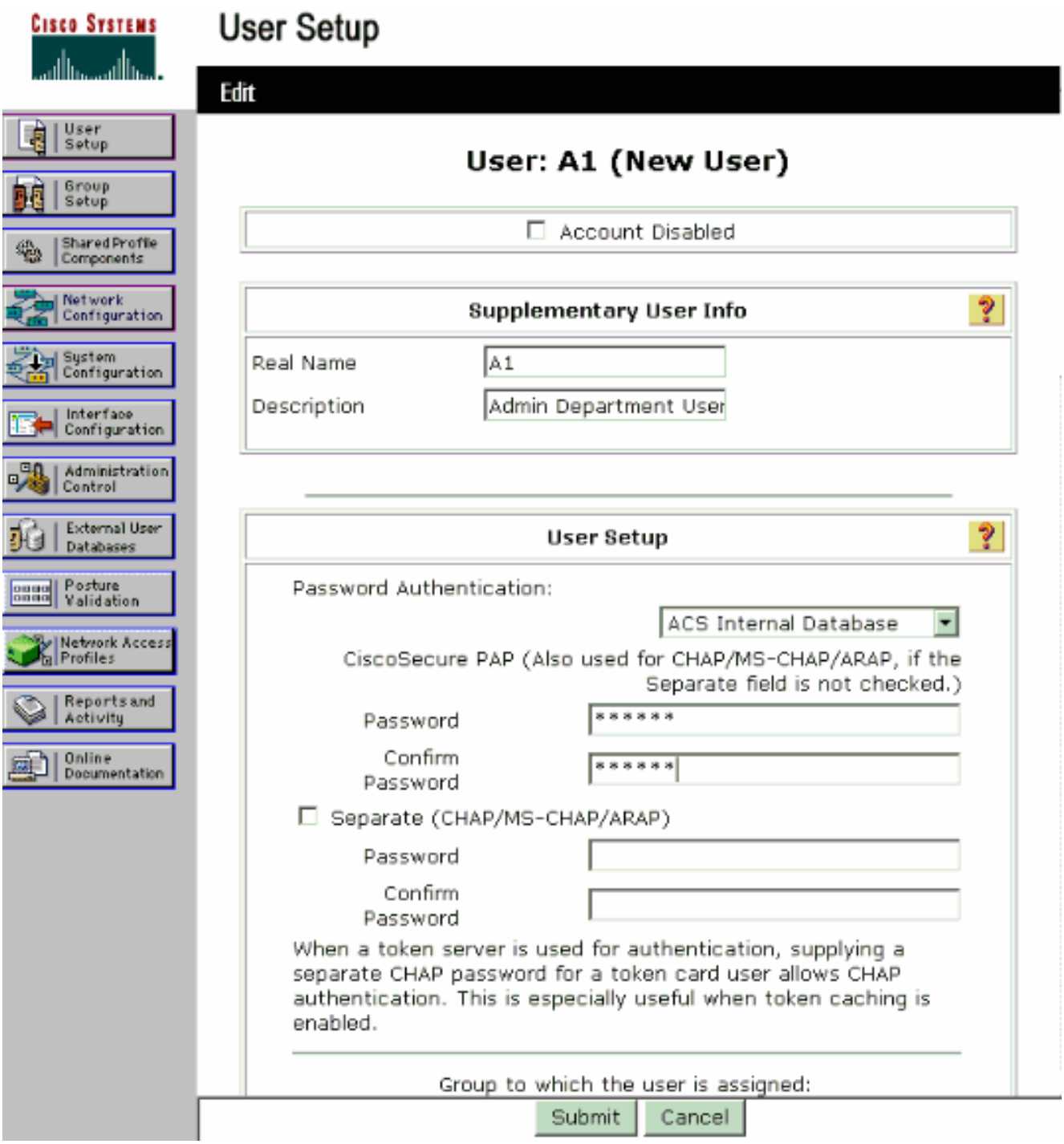
1. 为了将控制器定义为 ACS 服务器上的 AAA 客户端，请单击 ACS GUI 中的 **Network Configuration**。在 AAA Clients 下，单击 **Add Entry**。



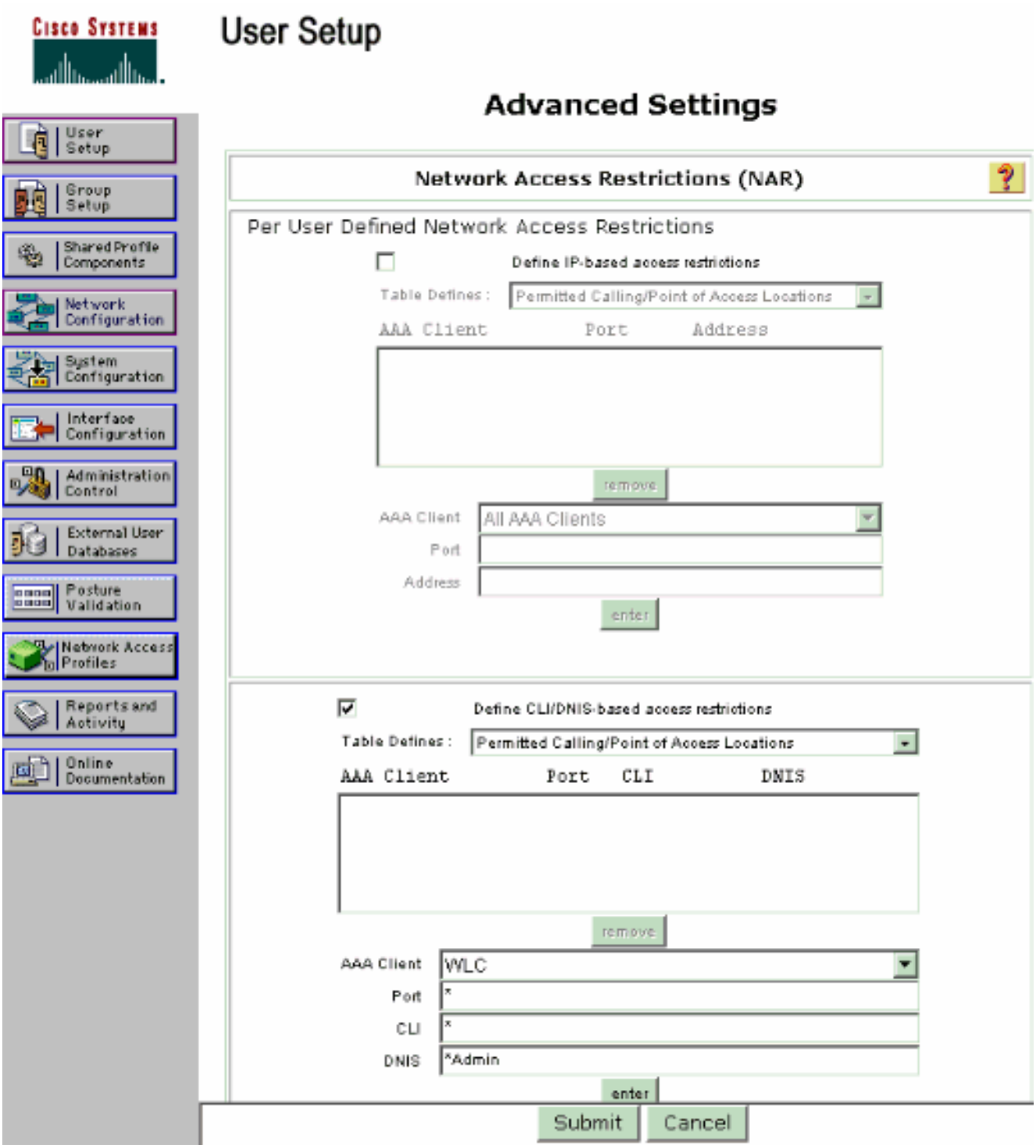
2. 出现 Network Configuration 页时，定义 WLC 的名称、IP 地址、共享密钥和身份验证方法 (RADIUS Cisco Airespace)。



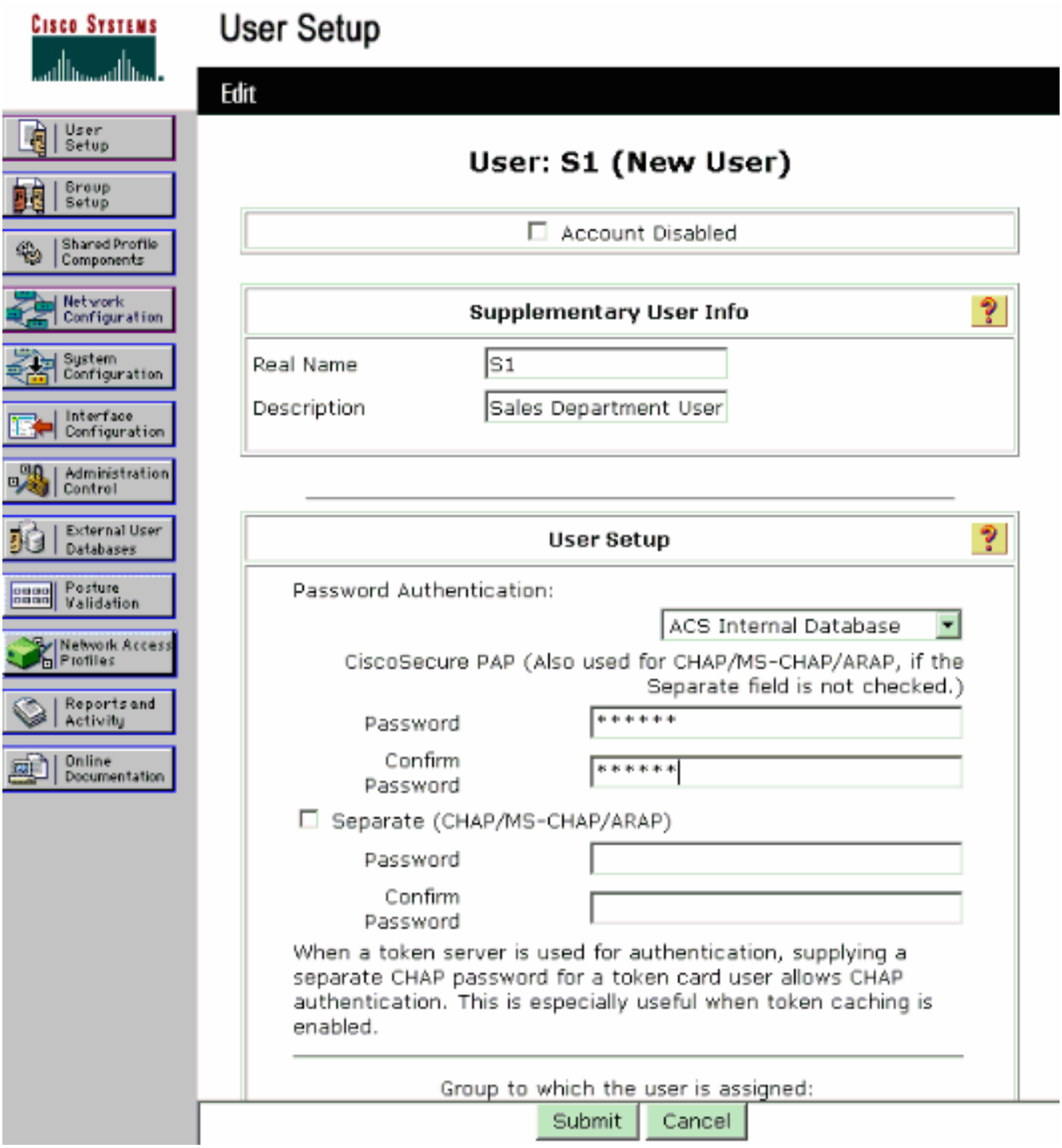
3. 在 ACS GUI 中单击 **User Setup**，输入用户名，然后单击 **Add/Edit**。本例中用户为 A1。
4. User Setup 页出现后，定义该用户特有的所有参数。本例中配置用户名、密码和附加用户信息，因为进行 LEAP 认证时需要这些参数。

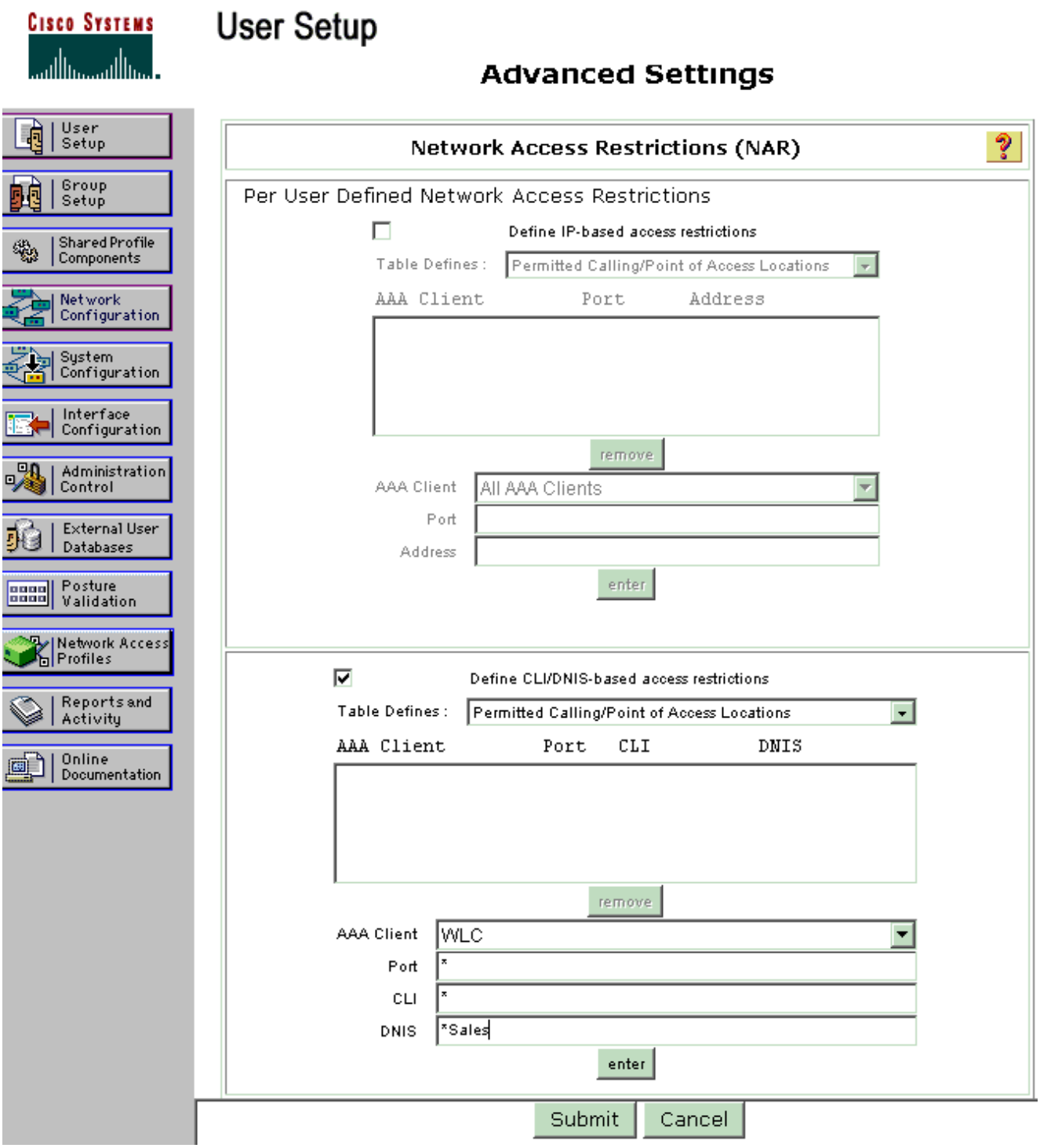


5. 向下滚动到 User Setup 页下方，直到您看到 Network Access Restrictions 部分。在 DNIS/CLI Access Restriction 用户界面下，选择 **Permitted Calling/Point of Access Locations** 并且定义以下参数：**AAA client** — WLC IP 地址（示例中为 172.16.1.30）**端口**— ***CLI** — ***DNIS** — *ssidname
6. DNIS 属性定义了允许用户访问的 SSID。WLC 将 DNIS 属性中的 SSID 发送到 RADIUS 服务器。如果用户仅需要访问名为 Admin 的 WLAN，请在 DNIS 字段中输入 ***Admin**。这可以确保用户仅访问名为 Admin 的 WLAN。单击 Enter。**Note:** SSID 务必以 **？开头。**这是强制要求。

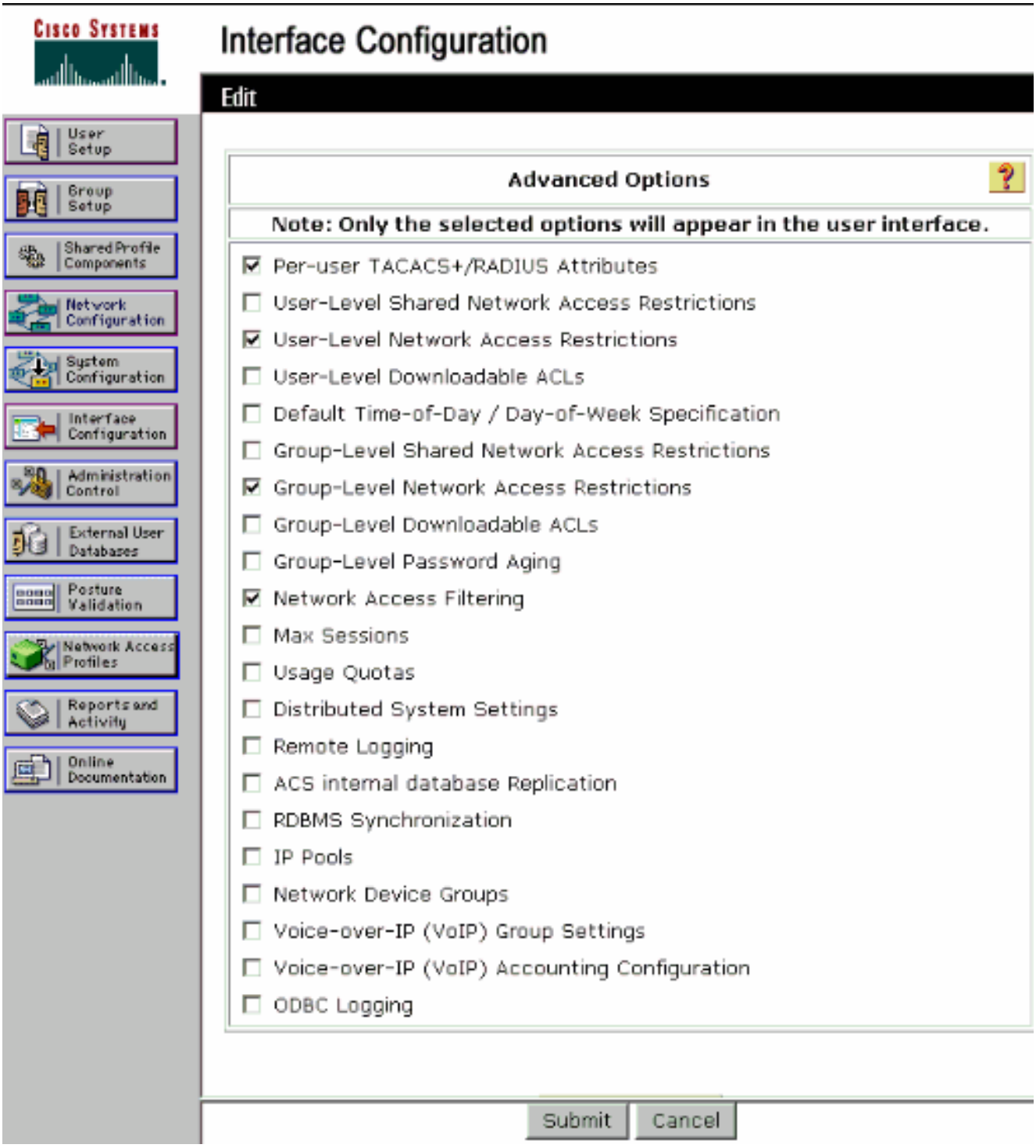


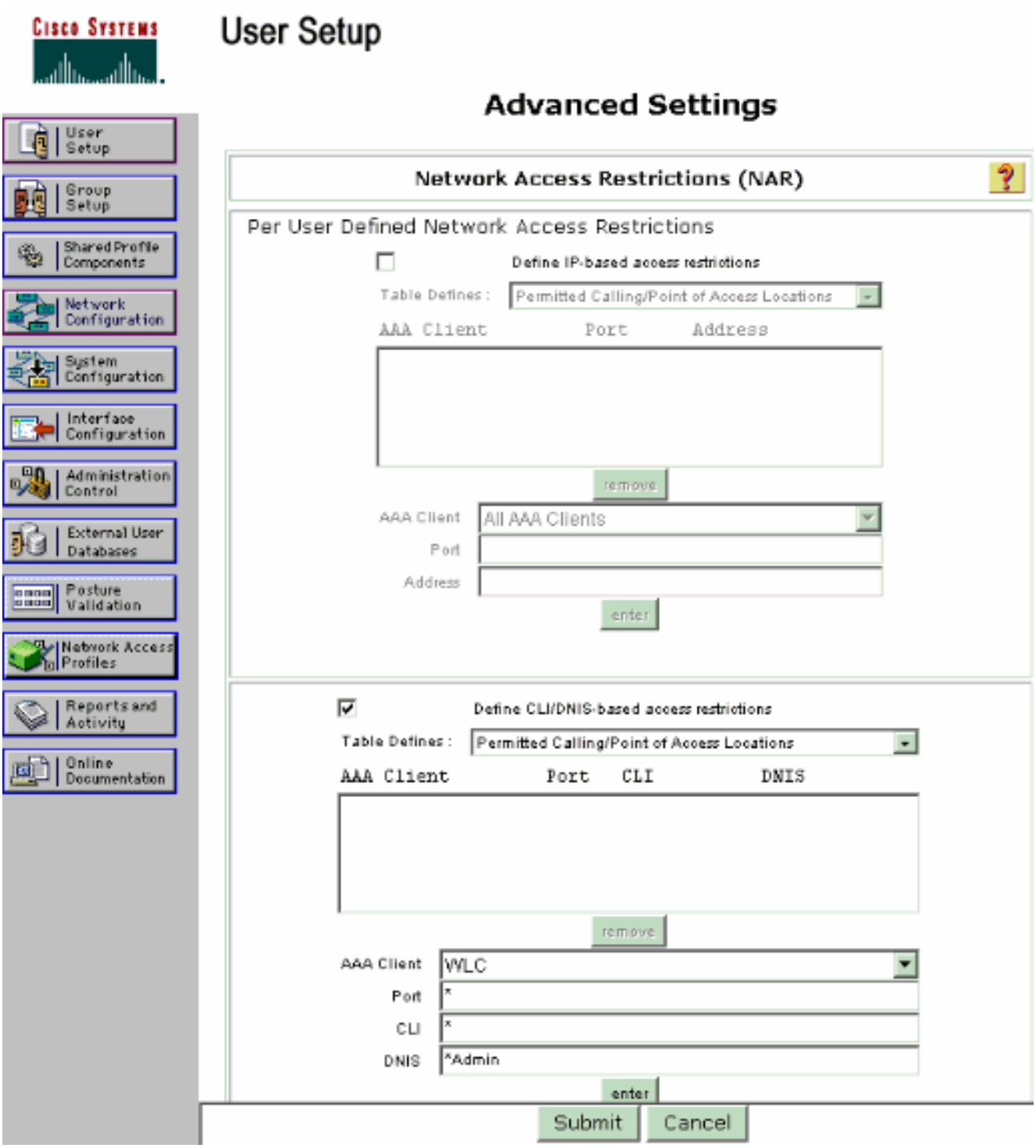
7. 单击 **submit**。
8. 以同样方式为销售部用户创建一个用户。以下是屏幕截图。


Cisco Systems
User Setup
Edit
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
User: S1 (New User)
Account Disabled
Supplementary User Info
Real Name
S1
Description
Sales Department User
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:
Submit
Cancel

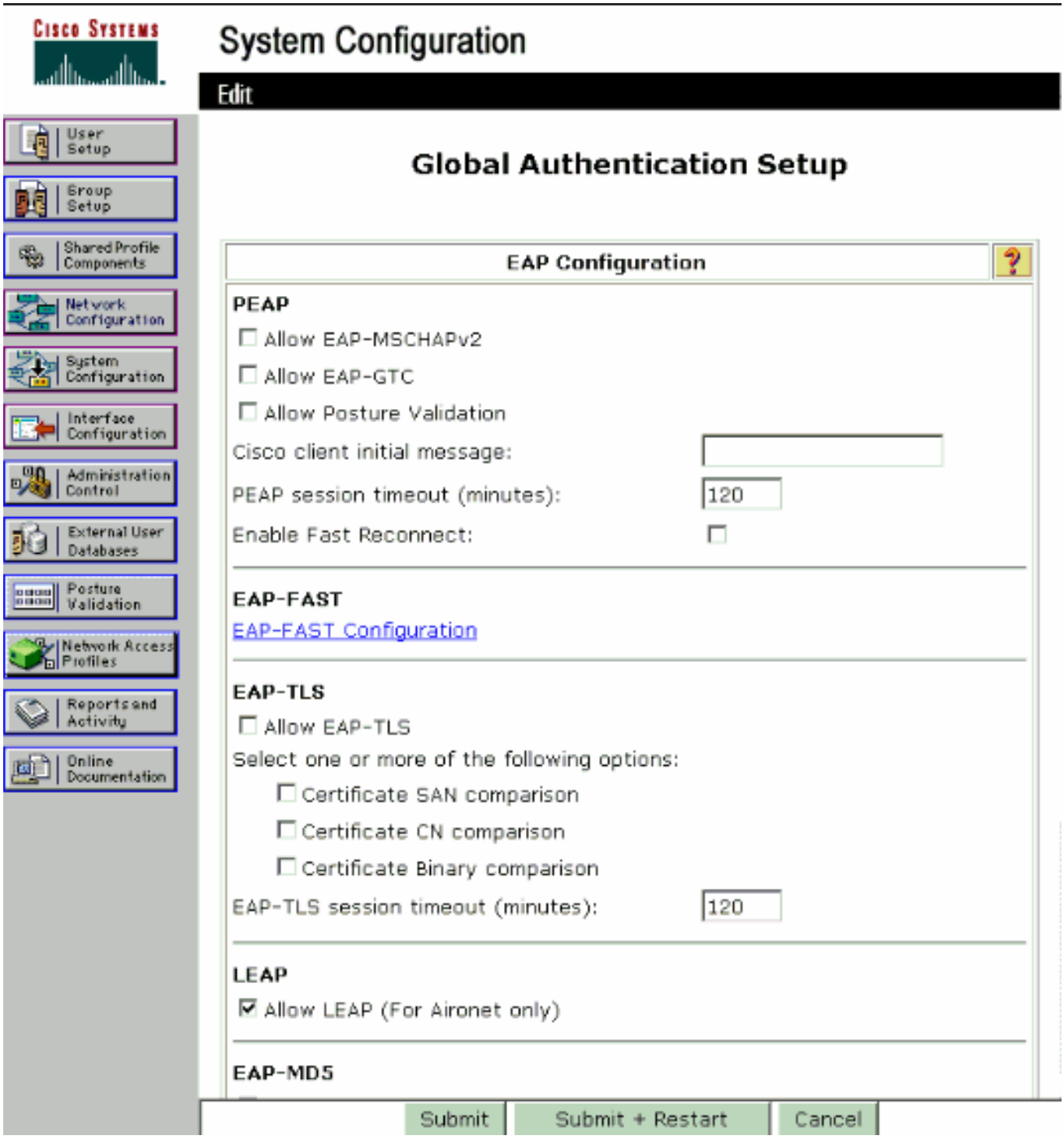


9. 重复同样的流程将更多用户添加到数据库。**Note:** 默认情况下，所有用户都会分配到默认组下。如果要将特定用户分配给不同组，请参阅适用于 Cisco Secure ACS 3.2 for Windows Server 用户指南的用户组管理部分。**Note:** 如果您在 User Setup 窗口中未看到 Network Access Restrictions 部分，可能是因为尚未启用。要为用户启用 Network Access Restrictions，请从 ACS GUI 选择 **Interfaces > Advanced Options**，然后选择 **User-Level Network Access Restrictions** 后单击 **Submit**。这将启用 NAR 并在 User Setup 窗口中显示。


Cisco Systems
Interface Configuration
Edit
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Advanced Options
Note: Only the selected options will appear in the user interface.
Per-user TACACS+/RADIUS Attributes
User-Level Shared Network Access Restrictions
User-Level Network Access Restrictions
User-Level Downloadable ACLs
Default Time-of-Day / Day-of-Week Specification
Group-Level Shared Network Access Restrictions
Group-Level Network Access Restrictions
Group-Level Downloadable ACLs
Group-Level Password Aging
Network Access Filtering
Max Sessions
Usage Quotas
Distributed System Settings
Remote Logging
ACS internal database Replication
RDBMS Synchronization
IP Pools
Network Device Groups
Voice-over-IP (VoIP) Group Settings
Voice-over-IP (VoIP) Accounting Configuration
ODBC Logging
Submit
Cancel



10. 要启用 EAP 认证，单击 **System Configuration** 和 **Global Authentication Setup** 以确保认证服务器配置为可执行所需的 EAP 认证方法。在 EAP 配置设置下，选择适当的 EAP 方法。此示例使用LEAP认证。完成后，单击 **Submit**。

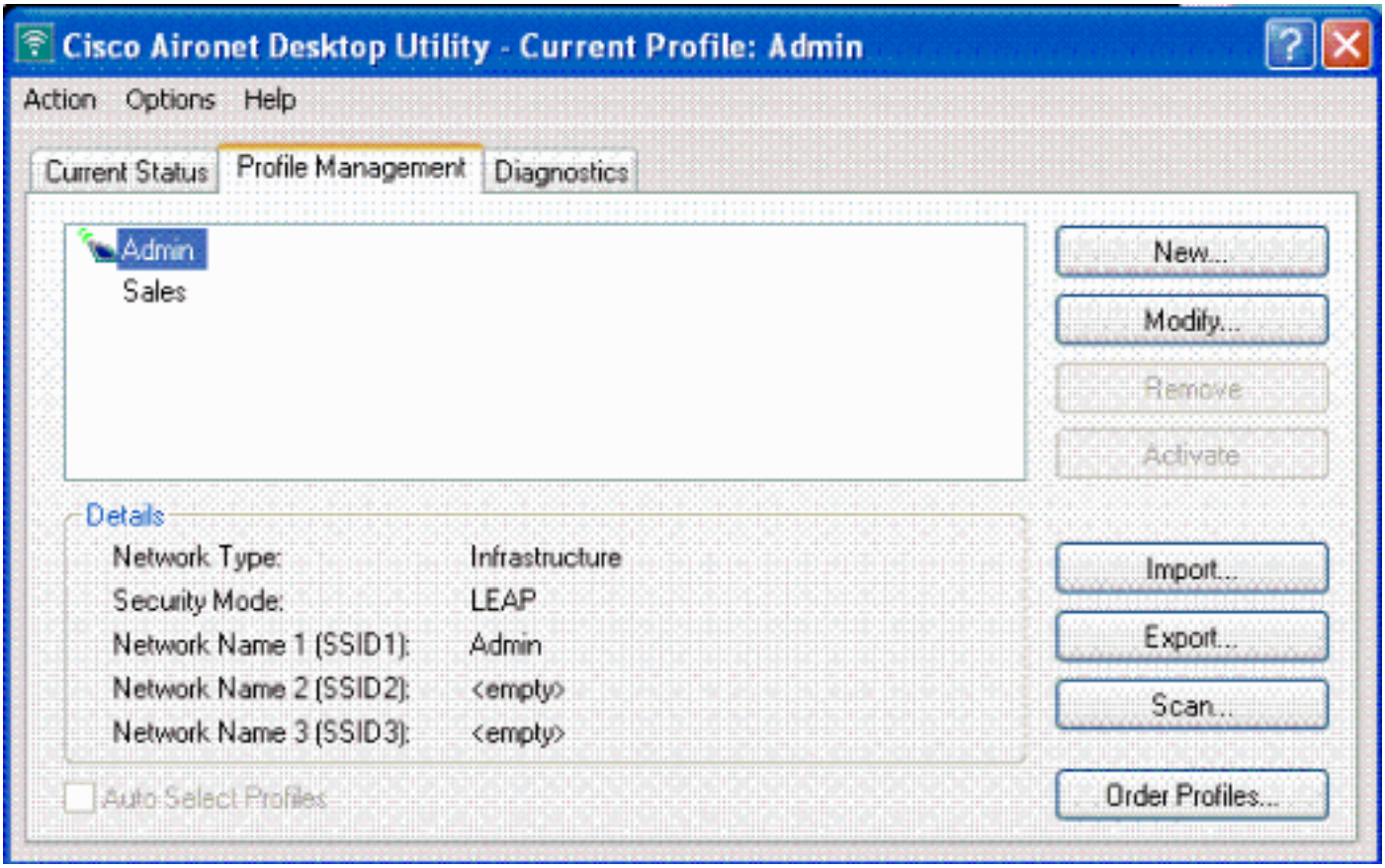


配置无线客户端并验证

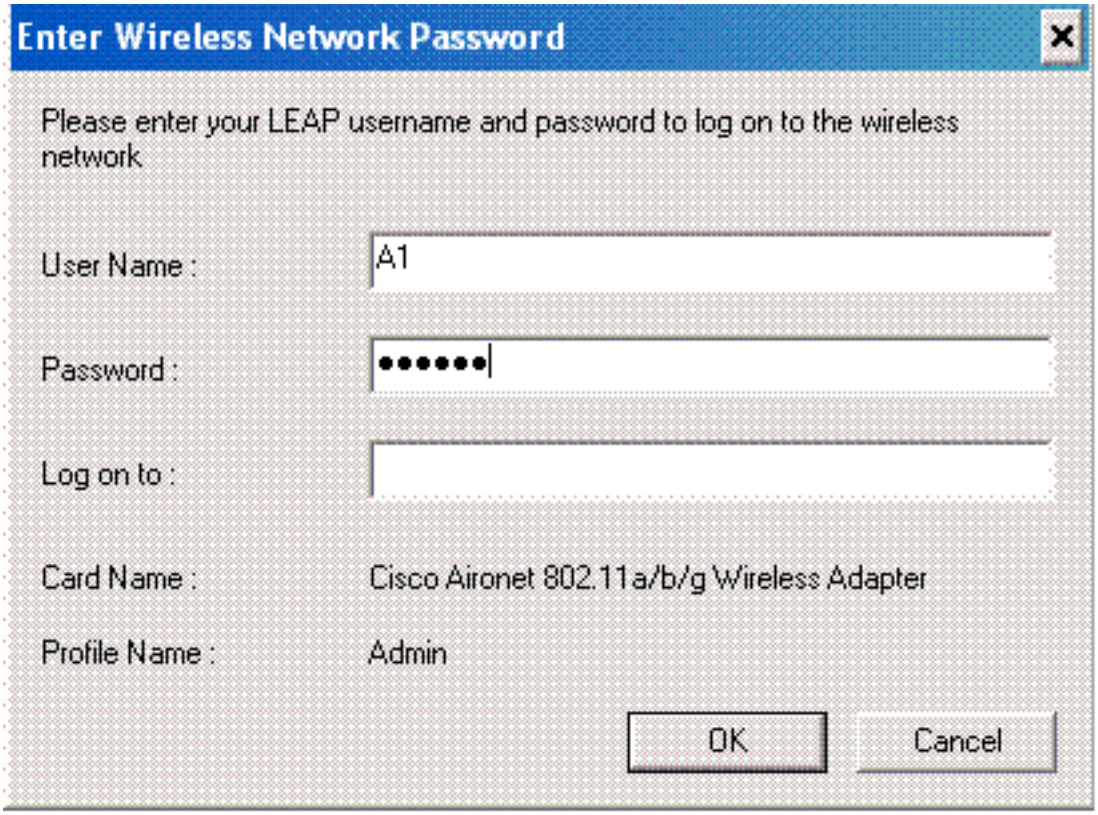
Use this section to confirm that your configuration works properly.尝试使用 LEAP 认证将无线客户端与 LAP 关联以验证该配置是否如期运行。

Note: 本文假设，客户端配置文件为LEAP认证被配置。有关如何为 LEAP 认证配置 802.11 a/b/g 无线客户端适配器的详细信息，请参阅使用 EAP 认证。

Note: 从 ADU 中，可以看到已配置的两个客户端配置文件。一个是适用于管理部门用户的，参数为 SSID **Admin**，另一个配置文件适用于销售部门用户，参数为 SSID **Sales**。两个配置文件都为 LEAP 认证配置。



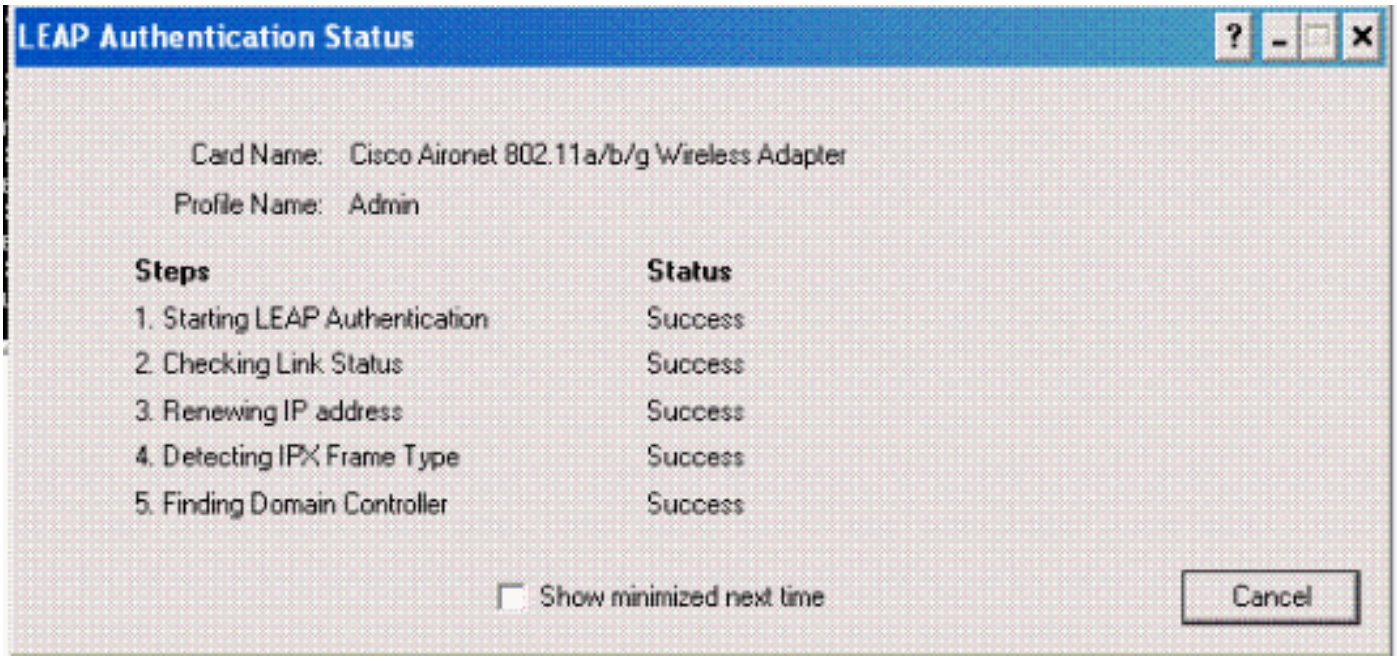
当来自管理部门的无线用户的配置文件激活时，要求用户提供用户名/密码用于 LEAP 验证。示例如下：



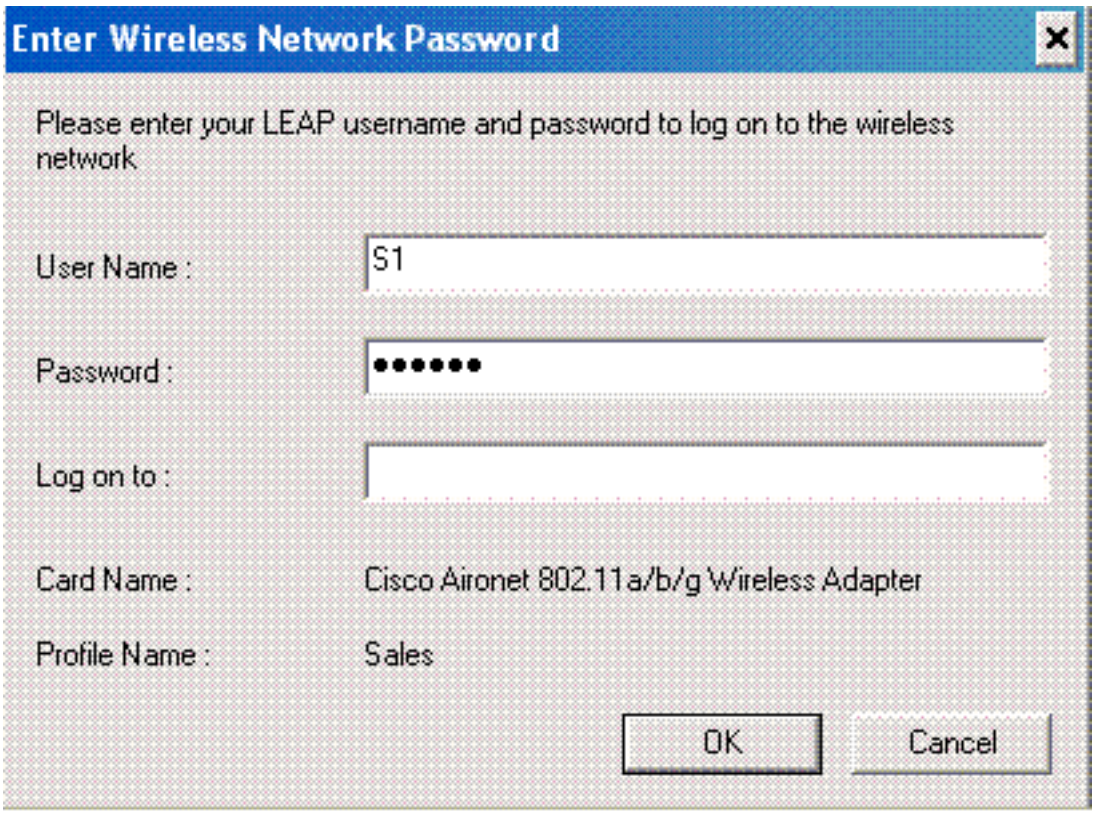
LAP 和 WLC 依次通过用户凭证到外部 RADIUS 服务器 (Cisco Secure ACS) 以验证凭证。WLC 将包括 DNIS 属性（SSID 名称）在内的凭证传递到 RADIUS 服务器用于验证。

RADIUS 服务器通过将数据与用户数据库（和 NAR）相比较来验证用户凭证，并在用户凭证有效时提供对无线客户端的访问权限。

RADIUS 认证成功后，无线客户端与 LAP 关联。



同样，当销售部门的用户激活销售配置文件时，用户由 RADIUS 服务器根据 LEAP 用户名/密码和 SSID 进行认证。



ACS 服务器的 Passed Authentication 报告显示客户端已通过 RADIUS 认证（EAP 认证和 SSID 认证）。示例如下：

Reports and Activity

Select

Passed Authentications active.csv Refresh Download

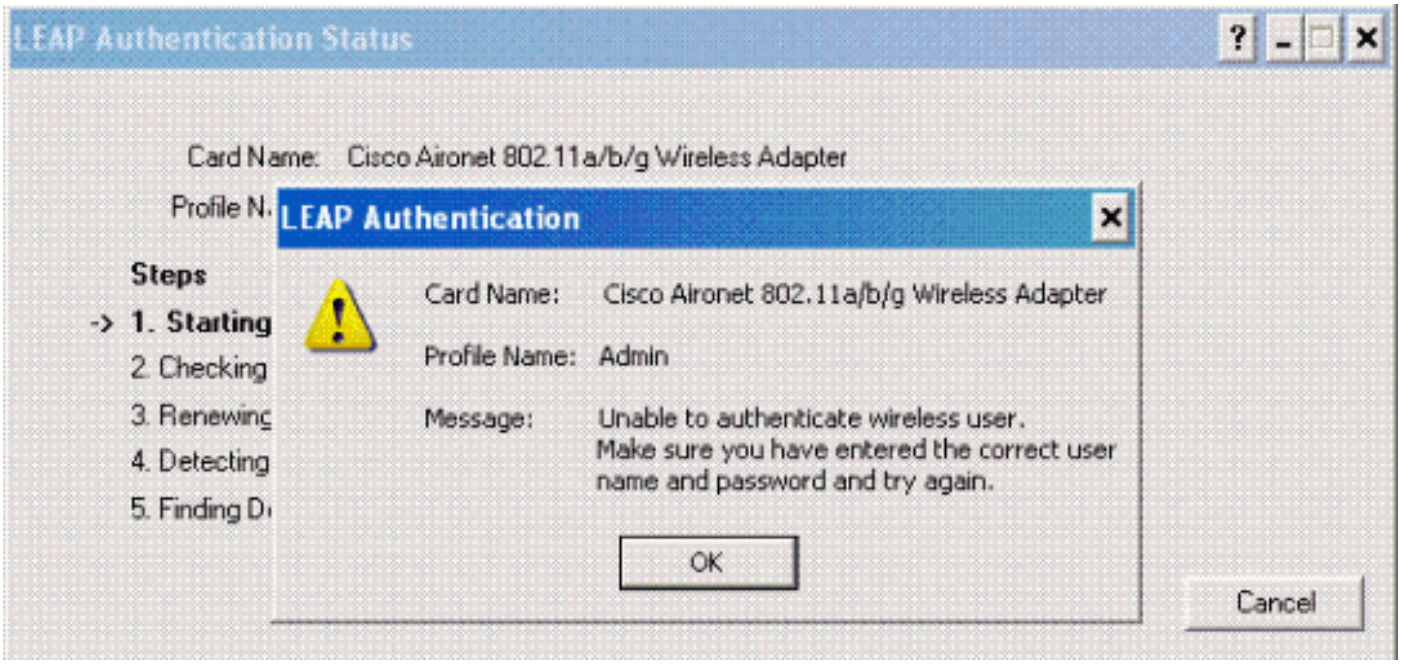
Regular Expression | Start Date & Time (mm/dd/yyyy,hh:mm:ss) | End Date & Time (mm/dd/yyyy,hh:mm:ss) | Rows per Page (50)

Apply Filter | Clear Filter

Filtering is not applied.

Date	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address	Network Access Profile Name	Shared RAC	Downloadable ACL	System-Posture-Token	Application-Posture-Token	Reason	EAP Type	EAP Type Name
10/11/2006	14:48:40	Authen OK	S1	Default Group	00-40-96-AC-E6-57	1	172.16.1.30	(Default)	..	..	..	..	..	17	LEAP
10/11/2006	14:47:05	Authen OK	A1	Default Group	00-40-96-AC-E6-57	1	172.16.1.30	(Default)	..	..	..	..	..	17	LEAP

现在，如果销售用户试图访问 **Admin** SSID，则 RADIUS 服务器将拒绝用户访问 WLAN。示例如下：



这样可基于 SSID 限制用户访问。在企业环境中，已划分到特定部门的用户可以分配到单个组并基于他们使用的 SSID 提供对 WLAN 的访问权限，如本文所述。

Troubleshoot

故障排除命令

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

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

- **debug dot1x aaa enable** — 启用 802.1x AAA 交互 debug。
- **debug dot1x packet enable** — 启用对所有 dot1x 数据包的调试。
- **debug aaa all enable** — 配置所有 AAA 消息的调试。

您还能使用 Cisco Secure ACS 服务器上的 Passed Authentication 报告和 Failed Authentication 报

告对配置进行故障排除。这些报告在 ACS GUI 上的 **Reports and Activity 窗口**下。

Related Information

- 与WLAN控制器(WLC)配置示例的EAP验证
- 无线局域网控制器 Web 身份验证配置示例
- 与无线局域网控制器配置示例的AP组VLAN
- 无线支持页
- Technical Support & Documentation - Cisco Systems