Cisco 统一无线网络的轻量级接入点(LAP)授权配置示例

目录

简介

本文解释如何配置无线局域网控制器(WLCs)授权根据拉普的MAC地址(拉普)的轻量级接入点。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 基础知识如何配置思科安全访问控制服务器(ACS)验证无线客户端
- Cisco Aironet拉普和思科WLCs的配置的知识
- 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Cisco 4400系列WLC
- Cisco Aironet 1000系列膝部
- Cisco Aironet 1200系列膝部
- Cisco Secure ACS服务器版本4.2

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。

轻量级接入点(LAP)授权

使用X.509证书，在LAP注册过程中，拉普和WLCs相互验证。

X.509证书烧录到在接入点(AP)和WLC的已保护闪存在出厂由思科。在AP，设立制造厂的证书呼叫制造安装的证书(MIC)。在七月AP被制造的所有思科18以后， 2005有MICs。

Cisco Aironet 1200， 1130和1240 AP被制造在七月18前， 2005年，从自治IOS升级到轻量级接入点协议(LWAPP) IOS，在升级进程中生成自签名证书(SSC)。关于如何管理与SSCs的AP的信息，参考升级对轻量级模式的自治Cisco Aironet接入点。

除在注册过程中发生的此相互验证之外， WLCs能也限制向他们登记根据LAP的MAC地址的拉普。

缺乏使用LAP的MAC地址的一强口令不应该是问题，因为控制器使用MIC在授权AP前验证AP通过RADIUS服务器。使用MIC提供强认证。

LAP授权在两种方式可以被执行：

- 使用在WLC的内部Authorization list
- 使用在AAA服务器的MAC地址数据库

拉普的行为有所不同基于使用的证书：

- 有SSCs的拉普— WLC只将使用内部Authorization list并且不是转发请求到这些拉普的一个RADIUS服务器。
- 拉普和MICs — WLC能使用在WLC配置的内部Authorization list或使用RADIUS服务器授权拉普

使用内部Authorization list和AAA服务器，本文讨论LAP授权。

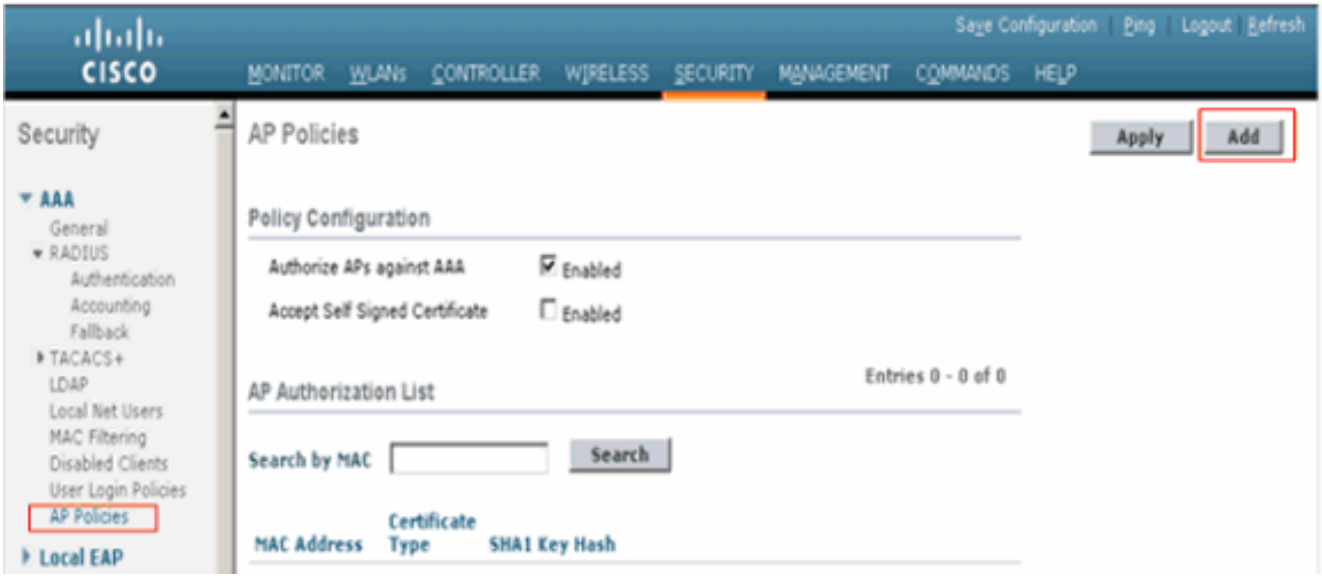
使用在WLC的内部Authorization list

在WLC，请使用AP authorization list限制根据他们的MAC地址的拉普。AP authorization list根据**安全> AP策略**是可用的在WLC GUI。

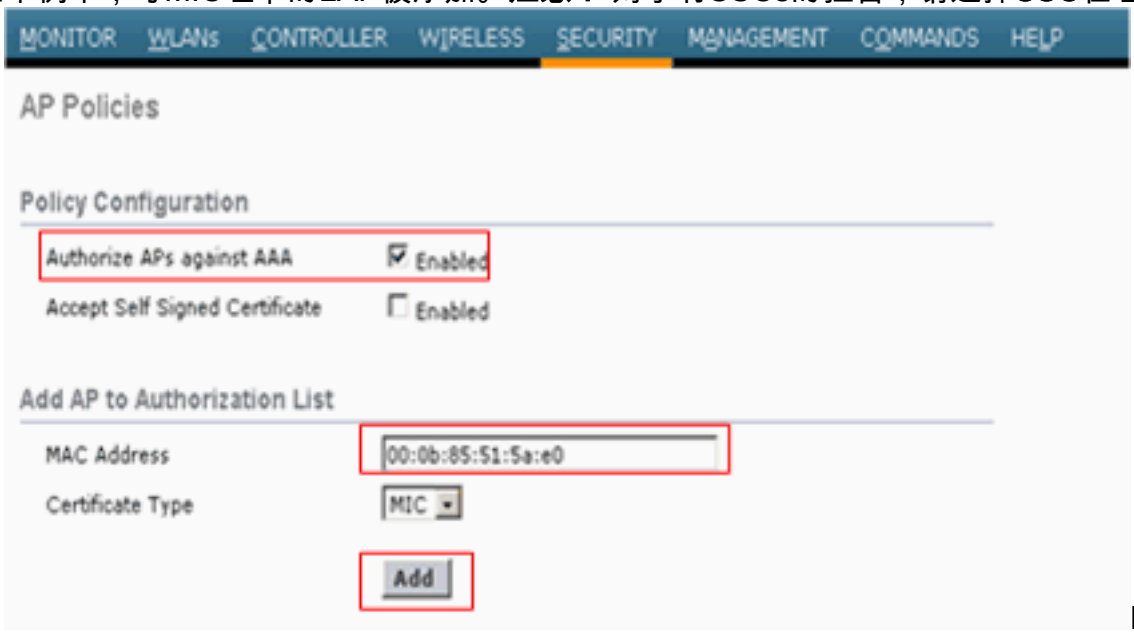
此示例如何显示添加与MAC地址**00:0b:85:5b:fb:d0的**LAP。

完成这些步骤：

1. 从WLC控制器GUI，请点击**安全> AP “Policies”**。Policies页的AP出现。
2. 在策略配置下，请检查方框**Authorize AP根据AAA**。当此参数选择时， WLC首先检查本地authorization list。如果LAP的MAC不存在，检查RADIUS服务器。
3. 点击**Add按钮**在屏幕的右边。



4. 下面请添加AP到Authorization list，输入AP MAC地址。然后，请选择证书类型并且单击**添加**。在本例中，与MIC证书的LAP被添加。**注意：** 对于有SSCs的拉普，请选择**SSC**在证书类型下。



LAP被添加到AP authorization list并且是列出的在**AP Authorization list**下。

验证

为了验证此配置，您需要连接与MAC地址00:0b:85:51:5a:e0的LAP对网络和监控。请使用**调试lwapp事件enable (event)**和**debug aaa所有enable (event)**命令执行此。

当LAP MAC地址不是存在AP authorization list时，此输出显示调试：

注意： 某些线路在输出中移动向第二行由于空间限制条件。

debug lwapp events enable Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 **Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'** Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 **Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1** Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1' Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1 Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 **Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'** Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:51:5A:E0 Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0 Wed Sep 12 17:42:50 2007: **spamRadiusProcessResponse: AP Authorization failure for 00:0b:85:51:5a:e0 debug aaa all enable** Wed Sep 12 17:56:26 2007: **Unable to find requested user entry for 000b85515ae0** Wed Sep 12 17:56:26 2007: AuthenticationRequest: 0xac476e8 Wed Sep 12 17:56:26 2007: Callback.....0x8108e2c Wed Sep 12 17:56:26 2007: protocolType.....0x00000001 Wed Sep 12 17:56:26 2007: proxyState.....00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:56:26 2007: Packet contains 8 AVPs (not shown) Wed Sep 12 17:56:26 2007: **00:0b:85:51:5a:e0 Returning AAA Error 'No Server' (-7) for mobile 00:0b:85:51:5a:e0** Wed Sep 12 17:56:26 2007: AuthorizationResponse: 0xbadff7d4 Wed Sep 12 17:56:26 2007: structureSize.....28 Wed Sep 12 17:56:26 2007: resultCode.....-7 Wed Sep 12 17:56:26 2007: protocolUsed.....0xffffffff Wed Sep 12 17:56:26 2007: proxyState.....00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:56:26 2007: Packet contains 0 AVPs: Wed Sep 12 17:56:31 2007: Unable to find requested user entry for 000b85515ae0 Wed Sep 12 17:56:31 2007: AuthenticationRequest: 0xac476e8 Wed Sep 12 17:56:31 2007: Callback.....0x8108e2c Wed Sep 12 17:56:31 2007: protocolType.....0x00000001 Wed Sep 12 17:56:31 2007: proxyState.....00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:56:31 2007: Packet contains 8 AVPs (not shown) Wed Sep 12 17:56:31 2007: 00:0b:85:51:5a:e0 Returning AAA Error 'No Server' (-7) for mobile 00:0b:85:51:5a:e0

当LAP的MAC地址被添加到AP authorization list时，此输出显示调试：

注意： 某些线路在输出中移动向第二行由于空间限制条件。

debug lwapp events enable Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 **Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'** Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 **Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1** Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 **Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1'** Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 **Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1** Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'** Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:51:5A:E0 Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0** Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 Successfully added NPU Entry for AP 00:0b:85:51:5a:e0 (index 58)Switch IP: 10.77.244.213, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 10.77.244.221, AP Port: 5550, next hop MAC: 00:0b:85:51:5a:e0 Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:51:5a:e0** Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1 debug aaa all enable** Wed Sep 12 17:57:44 2007: **User 000b85515ae0 authenticated** Wed Sep 12 17:57:44 2007: **00:0b:85:51:5a:e0 Returning AAA Error 'Success' (0) for mobile 00:0b:85:51:5a:e0** Wed Sep 12 17:57:44 2007: AuthorizationResponse: 0xbadff96c Wed Sep 12 17:57:44 2007: structureSize.....70 Wed Sep 12 17:57:44 2007: resultCode.....0 Wed Sep 12 17:57:44 2007: protocolUsed.....0x00000008 Wed Sep 12 17:57:44 2007: proxyState.....00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:57:44 2007: Packet contains 2 AVPs: Wed Sep 12 17:57:44 2007: AVP[01] Service-Type..... 0x00000065 (101) (4 bytes) Wed Sep 12 17:57:44 2007: AVP[02] Airespace / WLAN-Identifier..... 0x00000000 (0) (4 bytes)

AAA服务器的AP授权

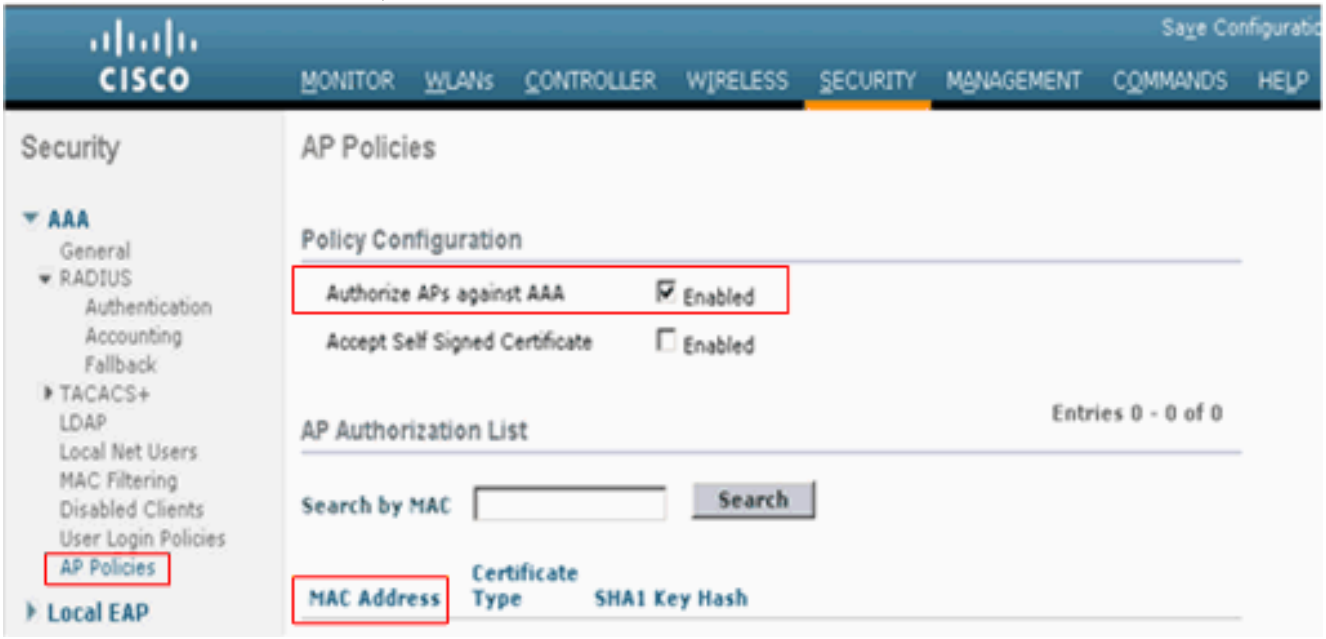
使用MICs，您能也配置WLCs使用RADIUS服务器授权AP。当发送信息对RADIUS服务器时，WLC使用LAP的MAC地址作为两个用户名和密码。例如，如果AP的MAC地址是000b85229a70，两个控制器用于的用户名和密码授权AP是000b85229a70。

注意： 如果使用MAC地址作为用户名和密码在RADIUS AAA服务器的AP验证，请勿使用同样AAA服务器客户端验证。对此的原因是，如果黑客发现AP MAC地址，然后他们能使用该MAC作为用户名和密码凭证获得在网络上。

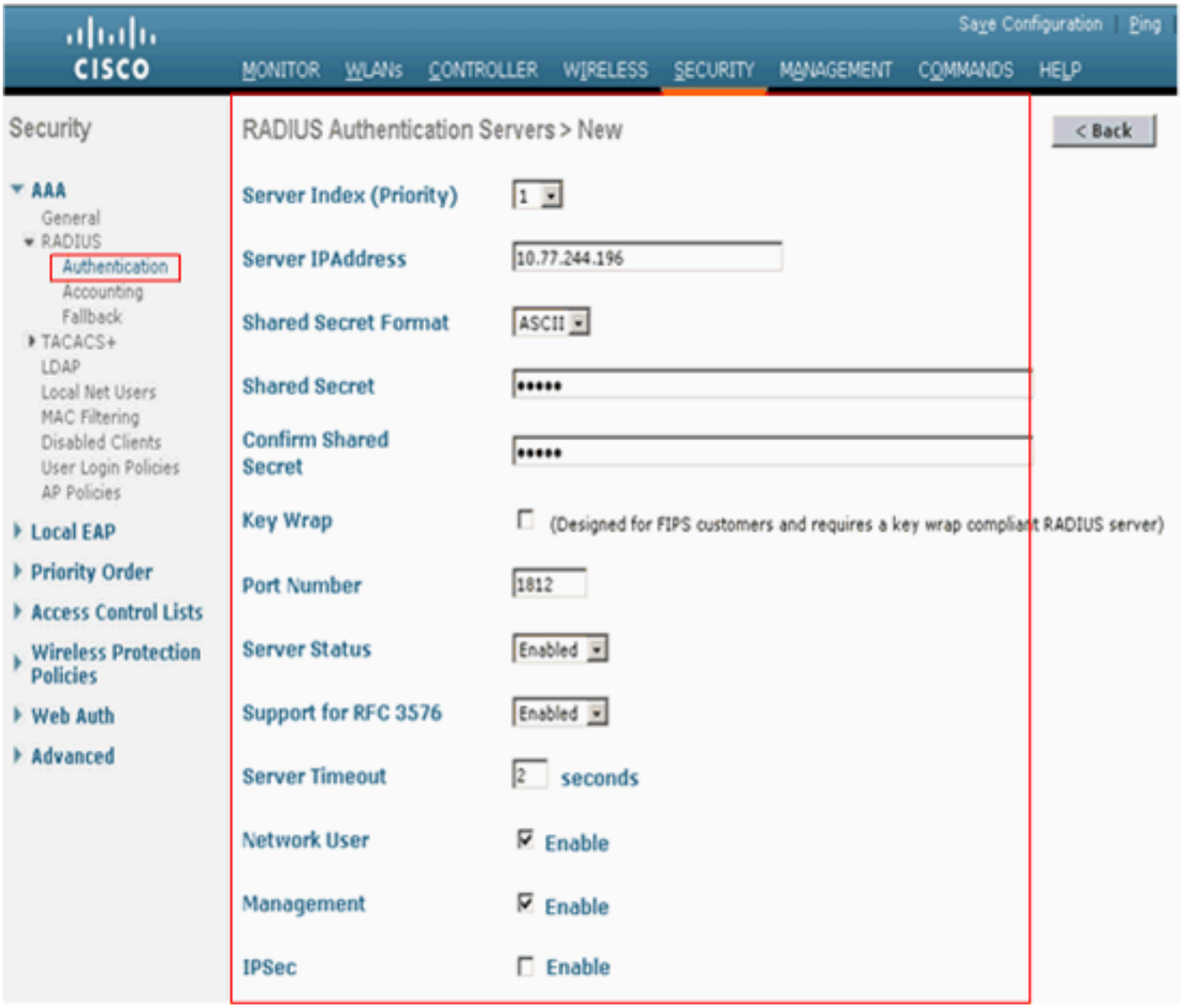
使用Cisco Secure ACS，此示例显示如何配置WLCs授权拉普。

在 WLC 上完成以下步骤：

1. 从WLC控制器GUI，请点击**安全> AP "Policies"**。Policies页的AP出现。
2. 在策略配置下，请检查方框**Authorize AP根据AAA**。当此参数选择时， WLC首先检查本地MAC数据库。为此，请确保本地数据库通过清除MAC地址是空的在AP Authorization list下。如果LAP MAC地址不存在，然后检查RADIUS服务器。



3. 在控制器的 GUI 中单击 **Security** 和"RADIUS Authentication"，以显示"RADIUS Authentication Servers"页。然后，请点击**new**来定义RADIUS服务器。



4. 在 **RADIUS Authentication Servers > New** 页上定义 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。此示例使用Cisco Secure ACS作为IP地址为10.77.244.196的 RADIUS服务器。
5. 单击 **Apply**。

配置Cisco Secure ACS授权拉普

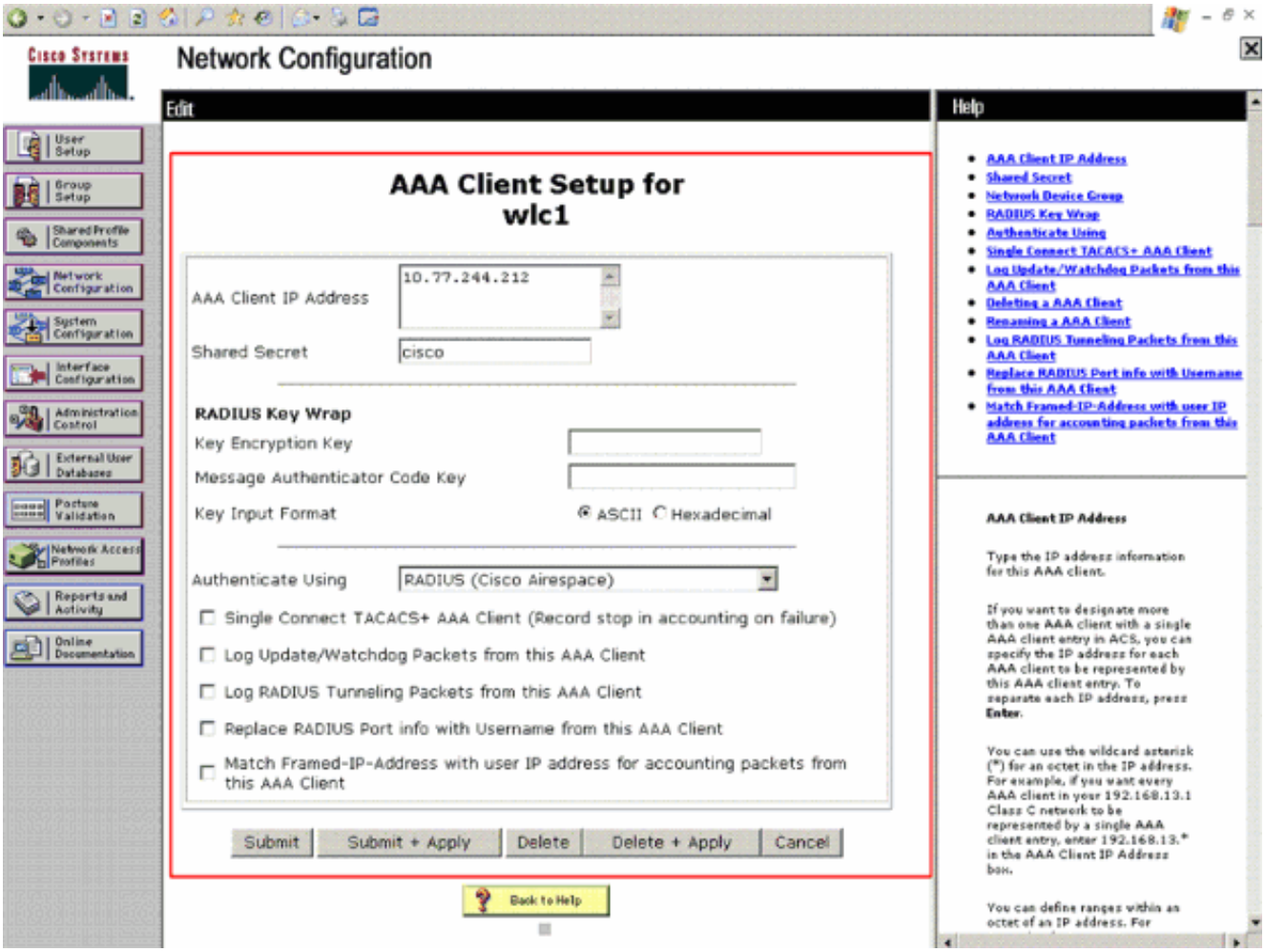
为了使Cisco Secure ACS授权拉普，您需要完成这些步骤：

1. 配置WLC作为Cisco Secure ACS的一个AAA客户端
2. 添加对用户数据库的LAP MAC地址在Cisco Secure ACS

配置WLC作为Cisco Secure ACS的AAA客户端

完成这些步骤为了配置WLC作为Cisco Secure ACS的一个AAA客户端：

1. 点击**Network Configuration >添加AAA客户端**。添加AAA客户端页出版。
2. 使用RADIUS Airespace，在此页，请定义WLC系统名称，管理接口IP地址，共享塞克雷，并且验证。**注意：** 或者，使用RADIUS Aironet，您能尝试验证选项。示例如下：

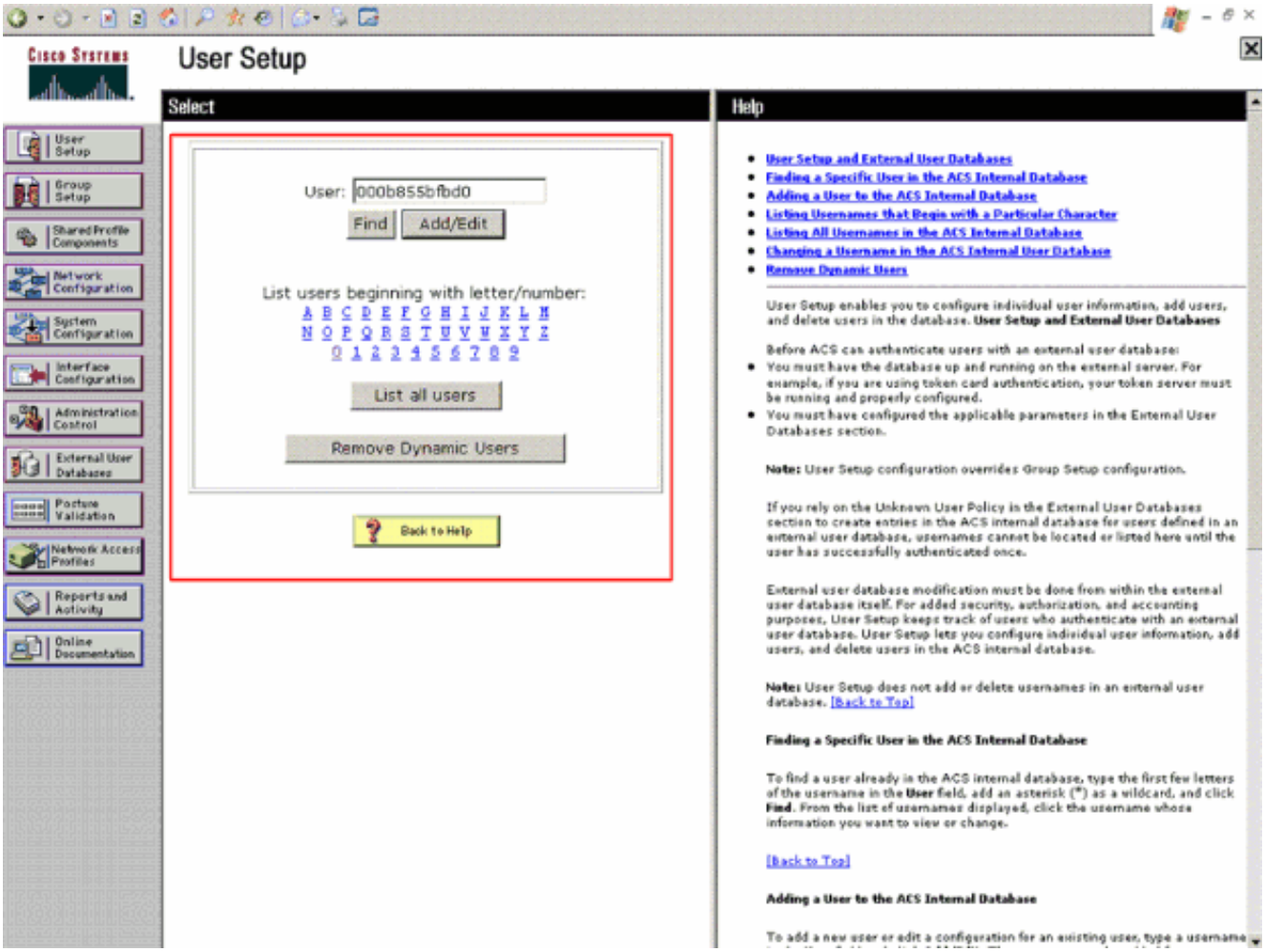


3. 单击 **Submit+Apply**。

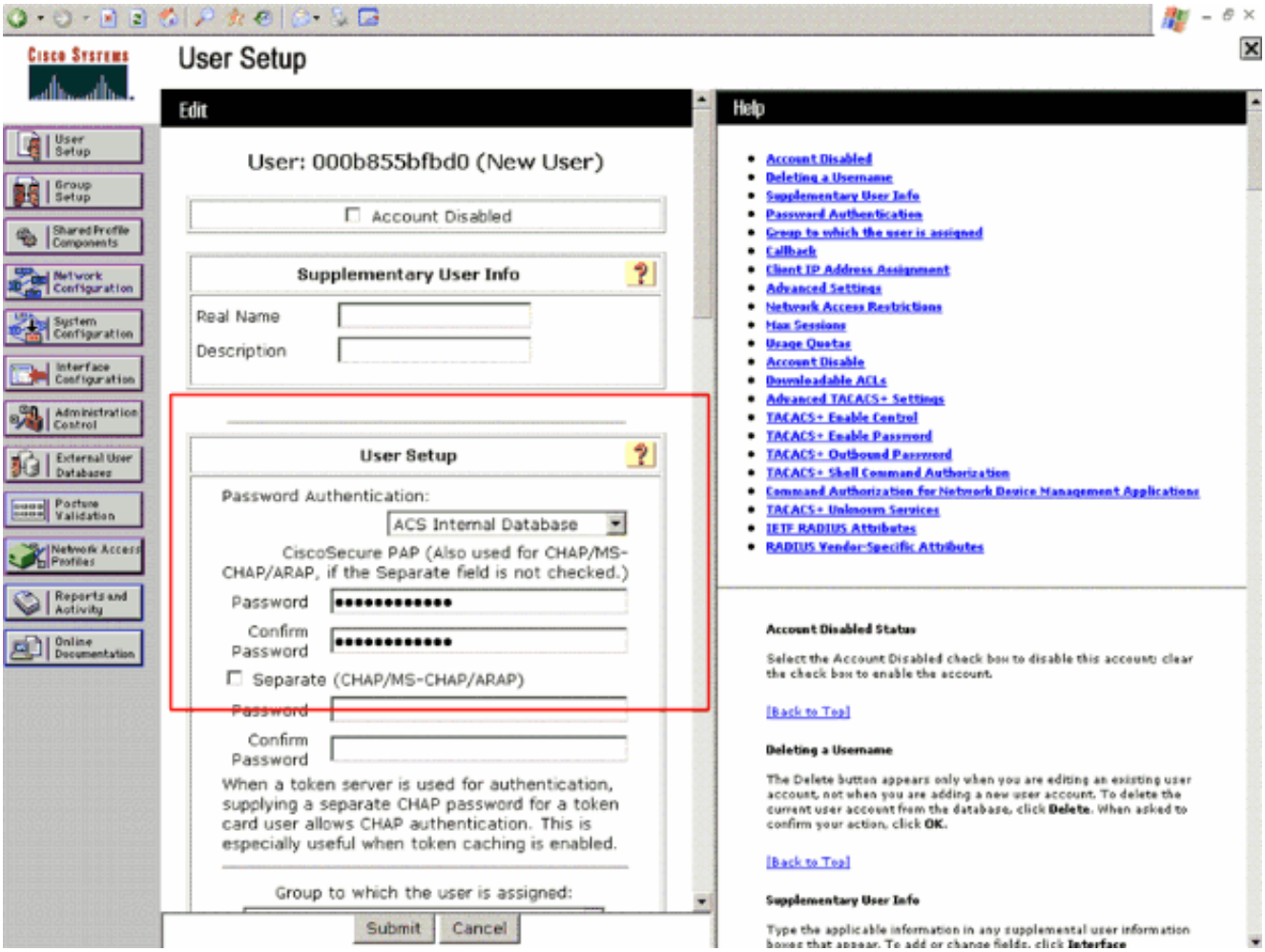
添加对用户数据库的LAP MAC地址在Cisco Secure ACS

完成这些步骤为了添加对Cisco Secure ACS的LAP MAC地址：

1. 从 ACS GUI 中选择 **User Setup**，输入用户名，然后单击 Add/Edit。用户名应该是您要授权LAP的MAC地址。MAC地址不能包含冒号或连字符。在本例中， LAP添加与MAC地址 **000b855bfbd0**
   ：



2. 当User Setup页出现时，请定义此LAP的密码在密码字段如显示。密码应该也是LAP的MAC地址。在本例中，它是**000b855bfbd0**。



3. 单击 **submit**。
4. 重复此步骤添加更多拉普对Cisco Secure ACS数据库。

验证

为了验证此配置，您需要连接与MAC地址00:0b:85:51:5a:e0的LAP对网络和监控。请使用**调试lwapp事件enable (event)**和**debug aaa所有enable (event)**命令为了执行此。

如被看到从调试，在对RADIUS服务器10.77.244.196的LAP MAC地址通过的WLC和服务器顺利地验证LAP。然后 LAP 注册到控制器。

注意： 某些线路在输出中移动向第二行由于空间限制条件。

```
debug aaa all enable Thu Sep 13 13:54:39 2007: AuthenticationRequest: 0xac48778 Thu Sep 13
13:54:39 2007: Callback.....................0x8108e2c Thu Sep 13 13:54:39 2007:
protocolType.....................0x00000001 Thu Sep 13 13:54:39 2007:
proxyState.....................00:0B:85:51:5A:E0-00:00 Thu Sep 13 13:54:39 2007: Packet
contains 8 AVPs (not shown) Thu Sep 13 13:54:39 2007: 00:0b:85:51:5a:e0 Successful transmission
of Authentication Packet (id 123) to 10.77.244.196:1812, proxy state 00:0b:85:51:5a:e0-85:51 Thu
Sep 13 13:54:39 2007: 00000000: 01 7b 00 72 00 00 00 00 00 00 00 00 00 00 00 00 .{.r............
Thu Sep 13 13:54:39 2007: 00000010: 00 00 00 00 01 0e 30 30 30 62 38 35 35 31 35 61
......000b85515a Thu Sep 13 13:54:39 2007: 00000020: 65 30 1e 13 30 30 2d 30 62 2d 38 35 2d 33
33 2d e0..00-0b-85-33- Thu Sep 13 13:54:39 2007: 00000030: 35 32 2d 38 30 1f 13 30 30 2d 30 62
2d 38 35 2d 52-80..00-0b-85- Thu Sep 13 13:54:39 2007: 00000040: 35 31 2d 35 61 2d 65 30 05 06
00 00 00 01 04 06 51-5a-e0..... Thu Sep 13 13:54:39 2007: 00000050: 0a 4d f4 d4 20 06 77 6c
63 31 02 12 03 04 0e 12 .M....wlc1..... Thu Sep 13 13:54:39 2007: 00000060: 84 9c 03 8f 63 40
2a be 9d 38 42 91 06 06 00 00 ....c@*..8B..... Thu Sep 13 13:54:39 2007: 00000070: 00 0a .. Thu
Sep 13 13:54:40 2007: 00000000: 02 7b 00 30 aa fc 40 4b fe 3a 33 10 f6 5c 30 fd .{.0..@K.:3..\0.
```

Thu Sep 13 13:54:40 2007: 00000010: 12 f3 6e fa 08 06 ff ff ff ff 19 16 43 41 43 53 ..n.....CACS Thu Sep 13 13:54:40 2007: 00000020: 3a 30 2f 39 37 37 2f 61 34 64 66 34 64 34 2f 31 :0/977/a4df4d4/1 Thu Sep 13 13:54:40 2007: ****Enter processIncomingMessages: response code=2 Thu Sep 13 13:54:40 2007: ****Enter processRadiusResponse: response code=2 Thu Sep 13 13:54:40 2007: **00:0b:85:51:5a:e0 Access-Accept received from RADIUS server 10.77.244.196 for mobile 00:0b:85:51:5a:e0** receiveId = 0 Thu Sep 13 13:54:40 2007: AuthorizationResponse: 0x9845500 Thu Sep 13 13:54:40 2007: structureSize.....84 Thu Sep 13 13:54:40 2007: resultCode.....0 Thu Sep 13 13:54:40 2007: protocolUsed.....0x00000001 Thu Sep 13 13:54:40 2007: proxyState.....00:0B:85:51:5A:E0-00:00 Thu Sep 13 13:54:40 2007: Packet contains 2 AVPs: Thu Sep 13 13:54:40 2007: AVP[01] Framed-IP-Address..... 0xffffffff (-1) (4 bytes) Thu Sep 13 13:54:40 2007: AVP[02] Class..... CACS:0/977/a4df4d4/1 (20 bytes) **debug lwapp events enable** Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 **Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'** Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1 Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1' Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 **Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1** Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1' Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:51:5A:E0 Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 **LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0** Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 Successfully added NPU Entry for AP 00:0b:85:51:5a:e0(index 57)Switch IP: 10.77.244.213, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 10.77.244.221, AP Port: 5550, next hop MAC: 00:0b:85:51:5a:e0 Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 **Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:51:5a:e0** Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 **Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1**

故障排除

请使用这些命令排除故障您的配置：

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

- **调试lwapp事件enable (event)** —配置LWAPP事件和错误调试。
- **调试lwapp数据包enable (event)** —配置LWAPP数据包踪迹调试。
- **调试所有启用**-的**aaa** Configures调试所有AAA消息。

相关信息

- 将自治 Cisco Aironet 接入点升级为轻量模式
- LWAPP升级工具故障排除提示
- 无线支持页
- 技术支持和文档 - Cisco Systems