Lightweight Access Point (LAP) Authorization in a Cisco Unified Wireless Network Configuration Example

Document ID: 98848

Introduction

This document explains how to configure Wireless LAN Controllers (WLCs) to authorize the Lightweight Access Points (LAPs) based on the MAC address of the LAPs.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Basic knowledge of how to configure a Cisco Secure Access Control Server (ACS) to authenticate wireless clients
- Knowledge of the configuration of Cisco Aironet LAPs and Cisco WLCs
- Knowledge of Cisco Unified Wireless Security Solutions

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 4400 Series WLC that runs Version 5.0.148.0
- Cisco Aironet 1000 series LAPs
- Cisco Aironet 1200 series LAPs
- Cisco Secure ACS Server Version 4.2

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.

Lightweight Access Point (LAP) Authorization

During the LAP registration process, the LAPs and WLCs mutually authenticate using X.509 certificates.

The X.509 certificates are burned into protected flash on both the access point (AP) and WLC at the factory by Cisco. On the AP, factory installed certificates are called manufacturing installed certificates (MIC). All Cisco APs manufactured after July 18, 2005 have MICs.

Cisco Aironet 1200, 1130, and 1240 APs manufactured before July 18, 2005, that have been upgraded from autonomous IOS to Lightweight Access Point Protocol (LWAPP) IOS, generate a self−signed certificate (SSC) during the upgrade process. For information on how to manage APs with SSCs, refer to Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode.

In addition to this mutual authentication that occurs during the registration process, the WLCs can also restrict the LAPs that register with them based on the MAC address of the LAP.

The lack of a strong password by the use of the LAP's MAC address should not be an issue because the controller uses MIC to authenticate the AP before authorizing the AP through the RADIUS server. The use of MIC provides strong authentication.

LAP authorization can be performed in two ways:

- Using the Internal Authorization list on the WLC
- Using the MAC address database on an AAA server

The behaviors of the LAPs differ based on the certificate used:

- LAPs with SSCs The WLC will only use the Internal Authorization list and will not forward a request to a RADIUS server for these LAPs.
- LAPs with MICs WLC can use either the Internal Authorization list configured on the WLC or use a RADIUS server to authorize the LAPs

This document discusses LAP authorization using both the Internal Authorization list and the AAA server.

Using the Internal Authorization List on the WLC

On the WLC, use the AP authorization list to restrict LAPs based on their MAC address. The AP authorization list is available under **Security > AP Policies** in the WLC GUI.

This example shows how to add the LAP with MAC address **00:0b:85:5b:fb:d0**.

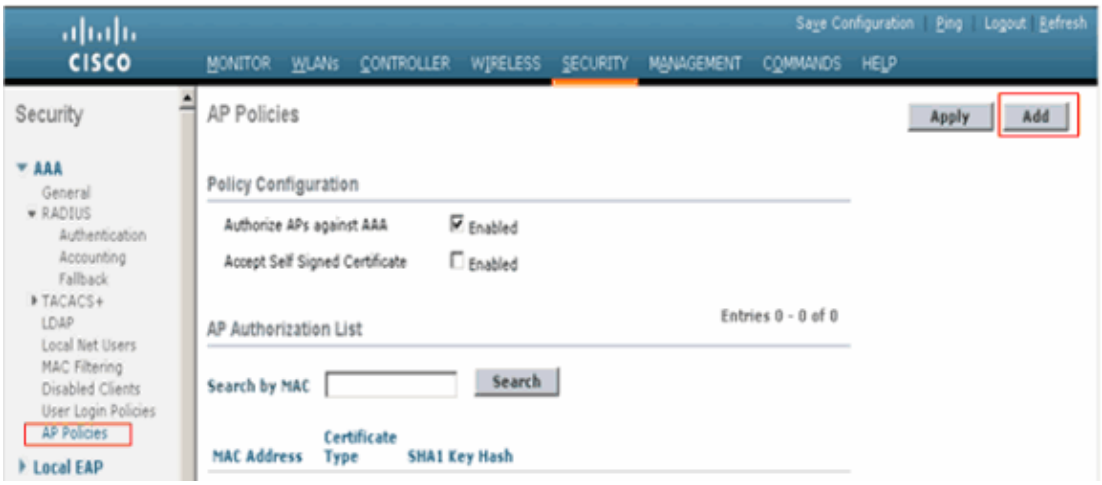
Complete these steps:

1. From the WLC controller GUI, click **Security > AP Policies**.

   The AP Policies page appears.
2. Under Policy Configuration, check the box for **Authorize APs against AAA**.

When this parameter is selected, the WLC checks the local authorization list first. If the LAP's MAC is not present, it checks the RADIUS server.

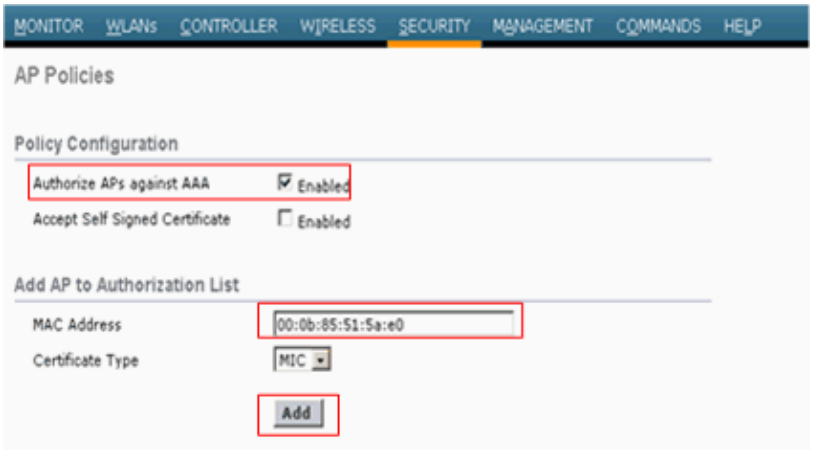
3. Click the **Add** button on the right hand side of the screen.



4. Under Add AP to Authorization List, enter the AP MAC address. Then, choose the certificate type and click **Add**.

   In this example, a LAP with MIC certificate is added.

   Note: For LAPs with SSCs, choose **SSC** under Certificate Type.



The LAP is added to the AP authorization list and is listed under **AP Authorization List**.

Verify

In order to verify this configuration, you need to connect the LAP with MAC address 00:0b:85:51:5a:e0 to the network and monitor. Use the **debug lwapp events enable** and **debug aaa all enable** commands to perform this.

This output shows the debugs when the LAP MAC address is not present in the AP authorization list:

Note: Some of the lines in the output have been moved to the second line due to space constraints.

```
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
```

This output show the debugs when the LAP's MAC address is added to the AP authorization list:

Note: Some of the lines in the output have been moved to the second line due to space constraints.

```
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)
```

AP Authorization Against an AAA Server

You can also configure WLCs to use RADIUS servers to authorize APs using MICs. The WLC uses a LAP's MAC address as both the username and password when sending the information to a RADIUS server. For example, if the MAC address of the AP is 000b85229a70, both the username and password used by the controller to authorize the AP are 000b85229a70.

Note: If you use the MAC address as the username and password for AP authentication on a RADIUS AAA server, do not use the same AAA server for client authentication. The reason for this is if hackers find out the AP MAC address, then they can use that MAC as the username and password credentials to get onto the network.

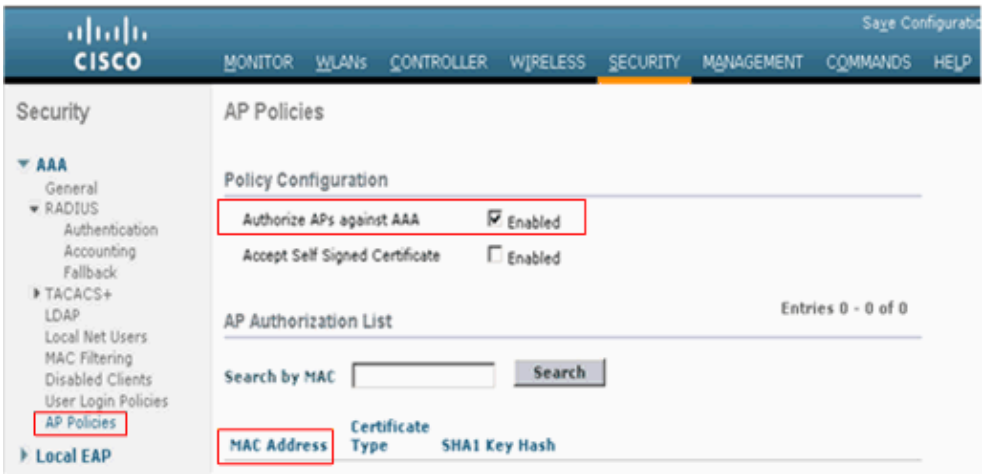
This example shows how to configure the WLCs to authorize LAPs using the Cisco Secure ACS.

Complete these steps on the WLC:

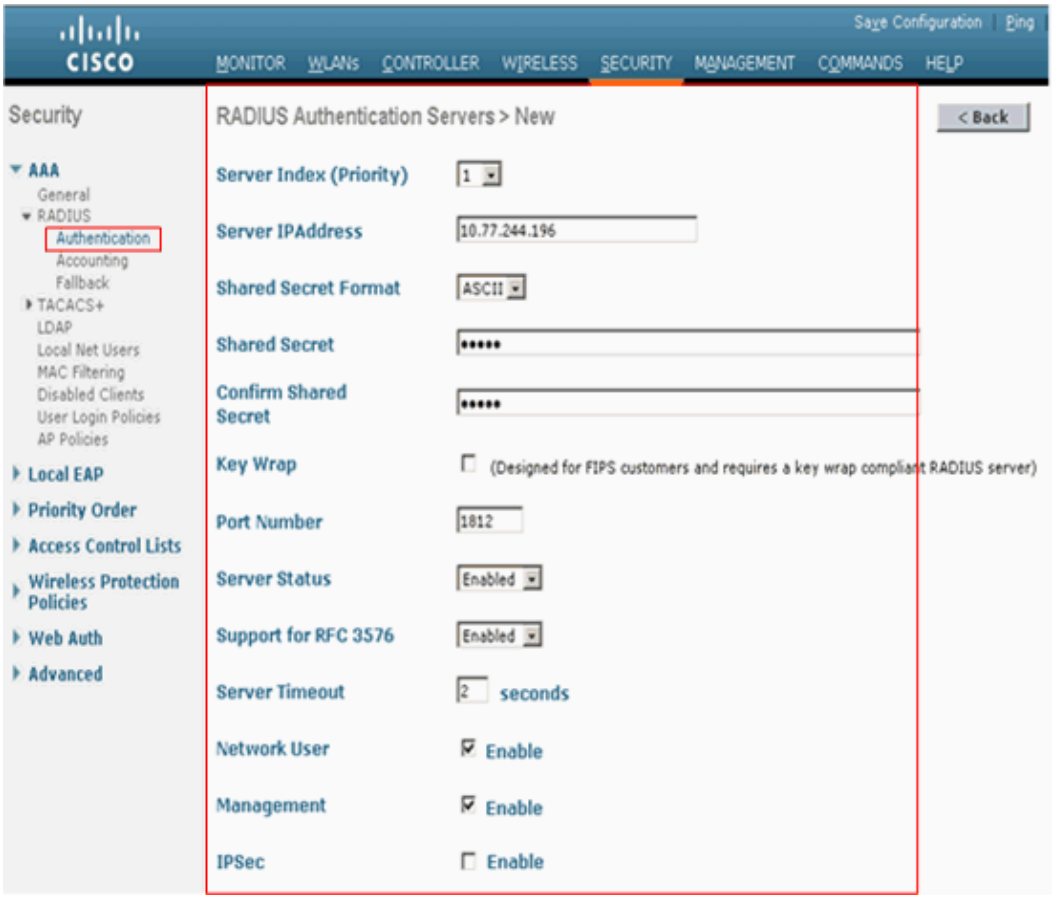
1. From the WLC controller GUI, click **Security** > **AP Policies**.

   The AP Policies page appears.
2. Under Policy Configuration, check the box for **Authorize APs against AAA**.

   When this parameter is selected, the WLC checks the local MAC database first. For this reason, make sure the Local database is empty by clearing the MAC addresses under the AP Authorization List . If the LAP MAC address is not present, it then checks the RADIUS server.



3. Click **Security** and **RADIUS Authentication** from the controller GUI to display the RADIUS Authentication Servers page. Then, click **New** in order to define a RADIUS server.



4. Define the RADIUS server parameters on the **RADIUS Authentication Servers > New** page. These parameters include the RADIUS Server IP Address, Shared Secret, Port Number, and Server Status.

   This example uses the Cisco Secure ACS as the RADIUS server with IP address 10.77.244.196.
5. Click **Apply**.

Configure the Cisco Secure ACS to Authorize LAPs

In order to enable the Cisco Secure ACS to authorize LAPs, you need to complete these steps:

1. Configure the WLC as an AAA Client on the Cisco Secure ACS
2. Add the LAP MAC Addresses to the User Database on the Cisco Secure ACS

Configure the WLC as an AAA Client on the Cisco Secure ACS

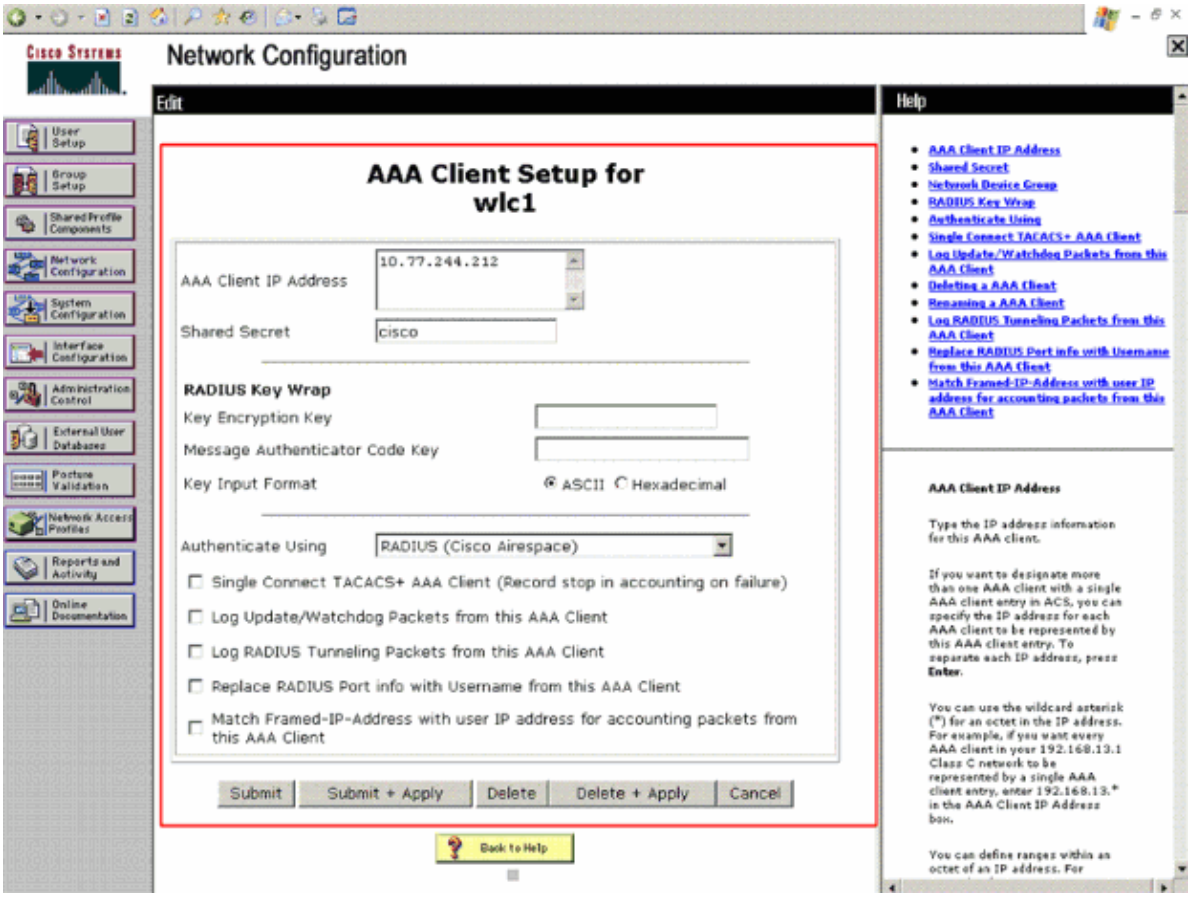
Complete these steps in order to configure the WLC as an AAA client on the Cisco Secure ACS:

1. Click **Network Configuration > Add AAA Client**.

   The Add AAA Client page appears.
2. On this page, define the WLC system name, Management Interface IP address, Shared Secret, and Authenticate Using RADIUS Airespace.

   Note: Alternatively, you can try the Authenticate option using RADIUS Aironet.

   Here is an example:



3. Click **Submit + Apply**.

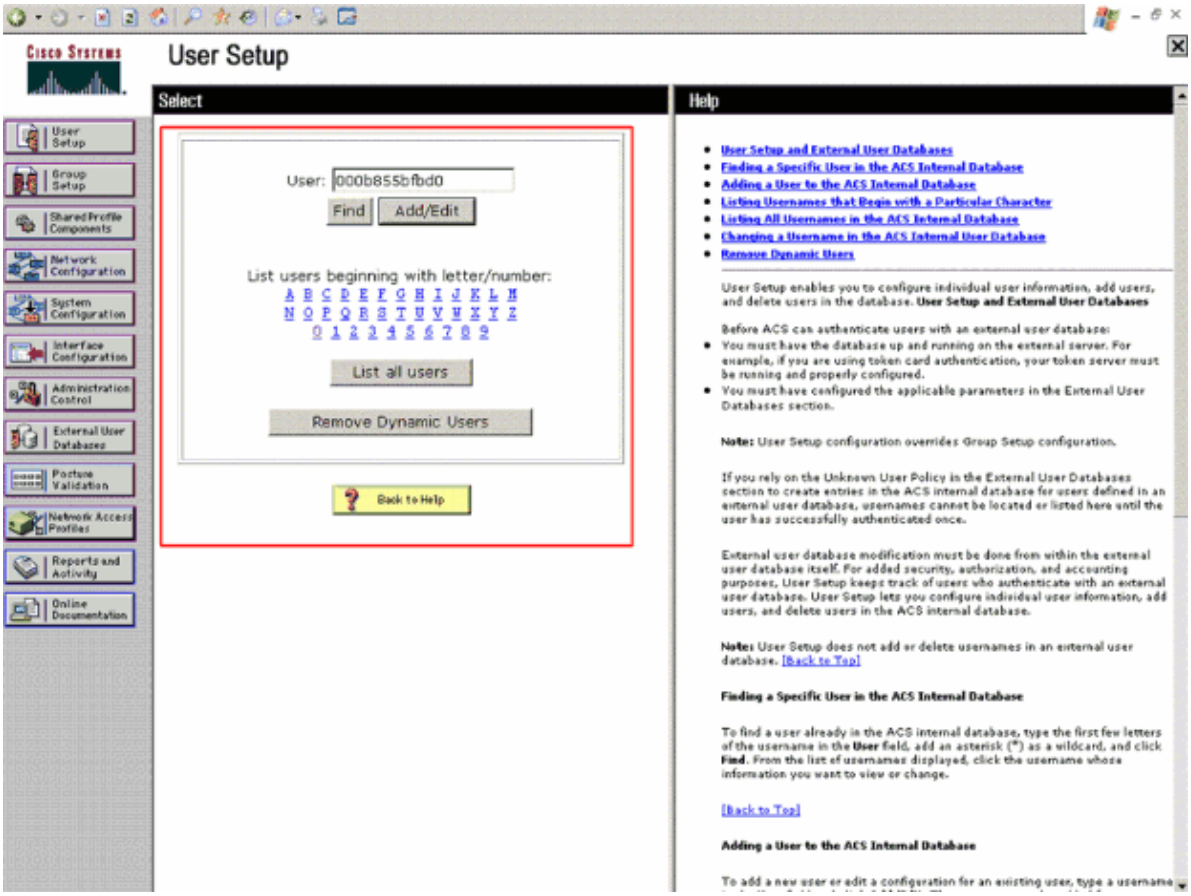
Add the LAP MAC Addresses to the User Database on the Cisco Secure ACS

Complete these steps in order to add the LAP MAC addresses to the Cisco Secure ACS:

1. Choose **User Setup** from the ACS GUI, enter the username, and click **Add/Edit**.

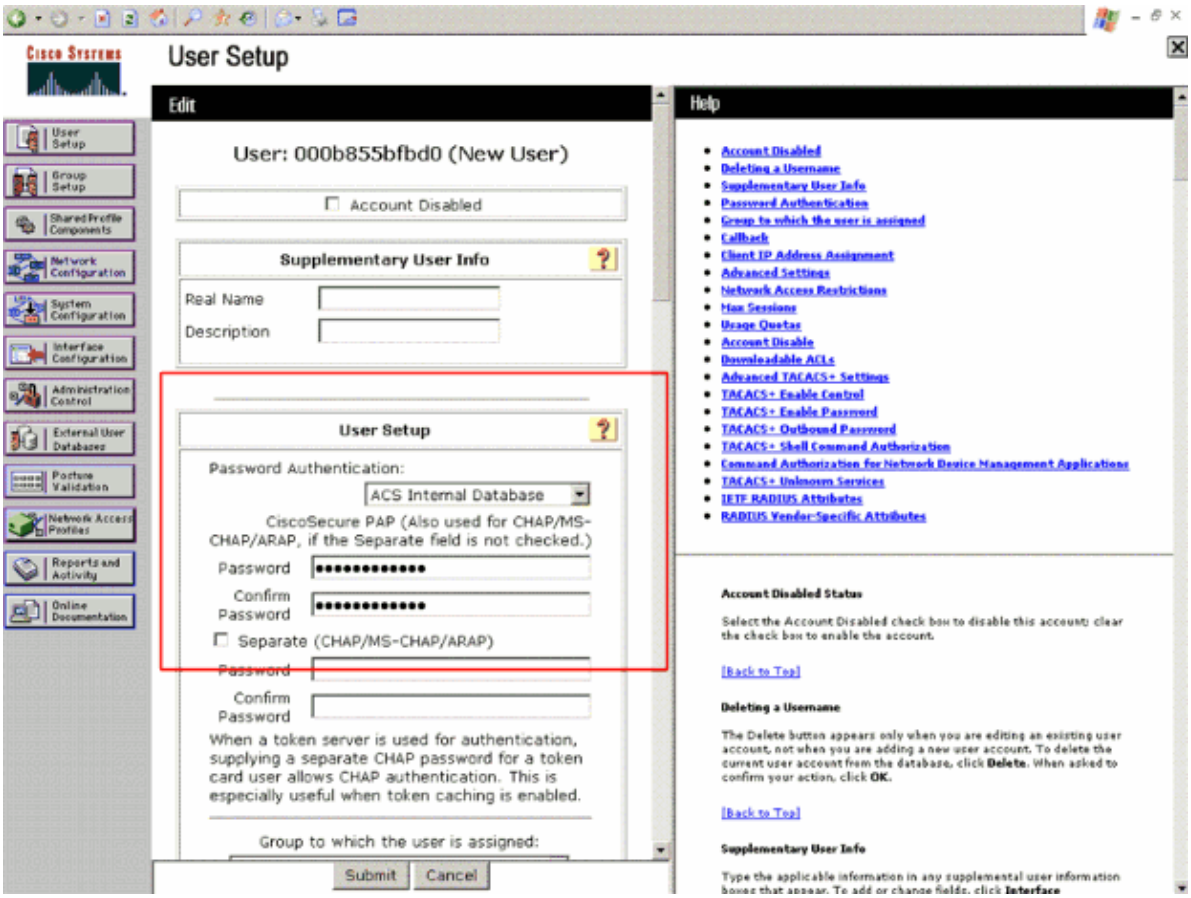
   The username should be the MAC address of the LAP that you want to authorize. The MAC address must not contain colons or hyphens.

   In this example, the LAP is added with MAC address **000b855bfbd0**:



2. When the User Setup page appears, define the password for this LAP in the password field as shown.

   The password should also be the LAP's MAC address. In this example, it is **000b855bfbd0**.



3. Click **Submit**.
4. Repeat this procedure to add more LAPs to the Cisco Secure ACS database.

Verify

In order to verify this configuration, you need to connect the LAP with MAC address 00:0b:85:51:5a:e0 to the network and monitor. Use the **debug lwapp events enable** and **debug aaa all enable** commands in order to perform this.

As seen from the debugs, the WLC passed on the LAP MAC address to the RADIUS server 10.77.244.196, and the server has successfully authenticated the LAP. The LAP then registers with the controller.

Note: Some of the lines in the output have been moved to the second line due to space constraints.

```
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
```

Troubleshoot

Use these commands to troubleshoot your configuration:

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug lwapp events enable** Configures debug of LWAPP events and errors.
- **debug lwapp packet enable** Configures debug of LWAPP Packet trace.
- **debug aaa all enable** Configures debug of all AAA messages.

Related Information

- **Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode**
- **LWAPP Upgrade Tool Troubleshoot Tips**
- **Wireless Support Page**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jun 02, 2009 Document ID: 98848