

# EAP Authentication with WLAN Controllers (WLC) Configuration Example

Document ID: 69730

---

## Introduction

### Prerequisites

- Requirements

- Components Used

- Conventions

### Configure

- Network Diagram

- Configure the WLC for Basic Operation and Register the Lightweight APs to the Controller

- Configure the WLC for RADIUS Authentication through an External RADIUS Server

- Configure WLAN Parameters

- Configure Cisco Secure ACS as the External RADIUS Server and Create a User Database for Authentication Clients

- Configure the Client

### Verify

### Troubleshoot

- Troubleshooting Tips

- Extracting the Package File from ACS RADIUS Server for Troubleshooting

### Related Information

---

## Introduction

This document explains how to configure the Wireless LAN controller (WLC) for Extensible Authentication Protocol (EAP) authentication with the use of an external RADIUS server. This configuration example uses the Cisco Secure Access Control Server (ACS) as the external RADIUS server in order to validate the user credentials.

## Prerequisites

### Requirements

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

- Basic knowledge of the configuration of Lightweight access points (APs) and Cisco WLCs.
- Basic knowledge of Lightweight AP Protocol (LWAPP)
- Knowledge of how to configure an external RADIUS server like the Cisco Secure ACS

### Components Used

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

- Cisco Aironet 1232AG Series Lightweight AP
- Cisco 4400 Series WLC that runs firmware 5.1
- Cisco Secure ACS that runs version 4.1
- Cisco Aironet 802.11 a/b/g Client Adapter

- Cisco Aironet Desktop Utility (ADU) that runs firmware 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.

## Configure

In this section, you are presented with the information to configure the features described in this document.

**Note:** Use the Command Lookup Tool ( registered customers only) in order to find more information on the commands used in this document.

Complete these steps in order to configure the devices for EAP authentication:

1. Configure the WLC for basic operation and register the Lightweight APs to the controller.
2. Configure the WLC for RADIUS authentication through an external RADIUS server.
3. Configure the WLAN parameters.
4. Configure Cisco Secure ACS as the external RADIUS server and create a user database for authenticating clients.

## Network Diagram

In this setup, a Cisco 4400 WLC and a Lightweight AP are connected through a hub. An external RADIUS server (Cisco Secure ACS) is also connected to the same hub. All the devices are in the same subnet. The AP is initially registered to the controller. You must configure the WLC and AP for Lightweight Extensible Authentication Protocol (LEAP) authentication. The clients that connect to the AP use LEAP authentication in order to associate with the AP. Cisco Secure ACS is used in order to perform RADIUS authentication.



## Configure the WLC for Basic Operation and Register the Lightweight APs to the Controller

Use the startup configuration wizard on the command-line interface (CLI) in order to configure the WLC for basic operation. Alternatively, you can also use the GUI in order to configure the WLC. This document explains the configuration on the WLC with the startup configuration wizard on the CLI.

After the WLC boots for the first time, it directly enters into the startup configuration wizard. Use the configuration wizard in order to configure basic settings. You can run the wizard on the CLI or the GUI. This output shows an example of the startup configuration wizard on the CLI:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC-1
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.77.244.204
Management Interface Netmask: 255.255.255.224
Management Interface Default Router: 10.77.244.220
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.77.244.220
AP Manager Interface IP Address: 10.77.244.205
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.77.244.220):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Test
Network Name (SSID): Cisco123
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configuration saved!
Resetting system with new configuration..
```

These parameters set up the WLC for basic operation. In this configuration example, the WLC uses **10.77.244.204** as the management interface IP address and **10.77.244.205** as the AP-manager interface IP address.

Before any other features can be configured on the WLCs, the Lightweight APs have to register with the WLC. This document assumes that the Lightweight AP is registered to the WLC. Refer to the Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC) for more information on how the Lightweight APs register with the WLC.

## Configure the WLC for RADIUS Authentication through an External RADIUS Server

The WLC needs to be configured in order to forward the user credentials to an external RADIUS server. The external RADIUS server then validates the user credentials and provides access to the wireless clients.

Complete these steps in order to configure the WLC for an external RADIUS server:

1. Choose **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.

Security

RADIUS Authentication Servers > Edit

Server Index: 1

Server Address: 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

Server Timeout: 2 seconds

Network User: ☒ Enable

Management: ☒ Enable

IPSec: ☐ Enable

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

The Network User and Management check boxes determine if the RADIUS–based authentication applies for WLC management and network users. This example uses the Cisco Secure ACS as the RADIUS server with IP address 10.77.244.196.

3. Radius server can now be used by the WLC for authentication. You can find the Radius Server listed if you choose **Security > Radius > Authentication**.

Security

RADIUS Authentication Servers

Call Station ID Type: IP Address

Use AES Key Wrap: ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	10.77.244.196	1812	Disabled	Enabled

RFC 3576 is supported on the Cisco CNS Access Registrar (CAR) RADIUS server, but not on Cisco Secure ACS Server version 4.0 and earlier.

You can also use the local RADIUS server feature in order to authenticate users. Local RADIUS server was introduced with version 4.1.171.0 code. WLCs that run previous versions do not have the local radius feature. Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users. Local EAP supports LEAP, EAP–FAST with PACs, EAP–FAST with certificates, and EAP–TLS authentication between the controller and wireless clients.

Local EAP is designed as a backup authentication system. If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients with the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured.

Refer to Local EAP Authentication on the Wireless LAN Controller with EAP–FAST and LDAP Server Configuration Example for more information on how to configure Local EAP on Wireless LAN controllers.

## Configure WLAN Parameters

Next, configure the WLAN which the clients use to connect to the wireless network. When you configured the basic parameters for the WLC, you also configured the SSID for the WLAN. You can use this SSID for the WLAN or create a new SSID. In this example, you create a new SSID.

**Note:** You can configure up to sixteen WLANs on the controller. The Cisco WLAN Solution can control up to sixteen WLANs for Lightweight APs. Each WLAN can be assigned unique security policies. Lightweight APs broadcast all active Cisco WLAN Solution WLAN SSIDs and enforce the policies that you define for each WLAN.

Complete these steps to configure a new WLAN and its related parameters:

1. Click **WLANs** from the GUI of the controller in order to display the WLANs page.

This page lists the WLANs that exists on the controller.

2. Choose **New** in order to create a new WLAN. Enter the Profile name and the WLAN SSID for the WLAN and click **Apply**. This example uses Cisco as the SSID.



The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs' (highlighted), 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANAGEMENT'. On the left, a sidebar shows 'WLANs' with a dropdown menu and 'Advanced' selected. The main content area is titled 'WLANs > New' and contains three fields: 'Type' with a dropdown menu set to 'WLAN', 'Profile Name' with a text box containing 'Cisco', and 'WLAN SSID' with a text box containing 'Cisco'.

3. Once you create a new WLAN, the WLAN > Edit page for the new WLAN appears. In this page you can define various parameters specific to this WLAN that includes General Policies, Security Policies, QOS policies and other Advanced parameters.

WLANs > Edit < Back

**General** **Security** **QoS** **Advanced**

Profile Name: Cisco

Type: WLAN

SSID: Cisco

Status: ☒ Enabled

Security Policies: [WPA2][Auth(802.1X)]  
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All

Interface: management

Broadcast SSID: ☒ Enabled

Choose the appropriate Interface from the drop-down menu. The other parameters can be modified based on the requirement of the WLAN network.

Check the **Status** box under General Policies in order to enable the WLAN.

- Click the **Security** tab and choose **Layer 2 Security**. From the Layer 2 Security drop-down menu, choose **802.1x**. In the 802.1x parameters, choose the WEP key size. This example uses 128-bit WEP key, which is the 104-bit WEP key plus the 24-bit Initialization vector.

WLANs > Edit

**General** **Security** **QoS** **Advanced**

**Layer 2** **Layer 3** **AAA Servers**

Layer 2 Security: 802.1X

☐ MAC Filtering

**802.1X Parameters**

802.11 Data Encryption	Type	Key Size
<input checked="" type="radio"/>	WEP	104 bits

- Choose the **AAA Servers** tab. From the Authentication Servers (RADIUS) drop-down menu, choose the appropriate RADIUS server. This server is used to authenticate the wireless clients.

WLANs > Edit

**General** **Security** **QoS** **Advanced**

**Layer 2** **Layer 3** **AAA Servers**

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

Radius Servers		LDAP Servers
Authentication Servers	Accounting Servers	
Server 1	IP:10.77.244.196, Port:1812	Server 1: None
Server 2	None	Server 2: None
Server 3	None	Server 3: None

**Local EAP Authentication**

Local EAP Authentication ☐ Enabled

6. Click **Apply** in order to save the configuration.

## Configure Cisco Secure ACS as the External RADIUS Server and Create a User Database for Authentication Clients

Complete these steps to create the user database and enable EAP authentication on the Cisco Secure ACS:

1. Choose **User Setup** from the ACS GUI, enter the username, and click **Add/Edit**. In this example the user is **ABC**.

**User Setup**

Select

User: ABC

Find Add/Edit

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

List All Users

Go to Help

**Help**

- [User Setup and External User Databases](#)
- [Finding a Specific User in the CiscoSecure User Database](#)
- [Adding a User to the CiscoSecure User Database](#)
- [Listing Usernames that Begin with a Particular Character](#)
- [Listing All Usernames in the CiscoSecure User Database](#)
- [Changing a Username in the CiscoSecure User Database](#)

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

**User Setup and External User Databases**

Before Cisco Secure 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 CiscoSecure user database for users defined in an external user database, username cannot be located or listed here until the user has successfully authenticated once.



2. When the User Setup page appears, define all the parameters specific to the user. In this example the username, password and Supplementary User Information are configured because you only need this parameters for EAP authentication.

Click **Submit** and repeat the same process in order to add more users to the database. By default all users are grouped under the default group and are assigned the same policy as defined for the group. Refer to the User Group Management section of User Guide for Cisco Secure ACS for Windows Server 3.2 for more information if you want to assign specific users to different groups.

The screenshot shows the 'User Setup' window in the Cisco Secure ACS GUI. The window is titled 'User: ABC (New User)'. It contains several sections: 'Account Disabled' (with a checkbox), 'Supplementary User Info' (with fields for 'Real Name' and 'Description'), and 'User Setup' (with a 'Password Authentication' section). The 'Password Authentication' section includes a dropdown menu set to 'CiscoSecure Database', a note about 'CiscoSecure PAP', and fields for 'Password', 'Confirm Password', and 'Separate (CHAP/MS-CHAP/ARAP)'. The 'Separate' section has fields for 'Password' and 'Confirm Password'. A note at the bottom explains that a separate CHAP password is used for token card authentication. On the right side, there is a 'Help' panel with a list of links including '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', and 'RADIUS Vendor-Specific Attributes'. At the bottom right, there is an 'Account Disabled Status' section with instructions on how to disable or enable the account and a '(Back to Top)' link. The 'Submit' and 'Cancel' buttons are at the bottom center.

3. Define the controller as an AAA client on the ACS server. Click **Network Configuration** from the ACS GUI.

When the Network Configuration page appears, define the name of the WLC, IP address, shared secret and authentication method (RADIUS Cisco Airespace). Refer to the documentation from the manufacturer for other non-ACS authentication servers.

**Note:** The shared secret key that you configure on the WLC and the ACS server must match. The shared secret is case sensitive.



## Add AAA Client

AAA Client Hostname	<input type="text" value="WLC-1"/>
AAA Client IP Address	<input type="text" value="10.77.244.204"/>
Shared Secret	<input type="text" value="cisco"/>

---

**RADIUS Key Wrap**

Key Encryption Key	<input type="text"/>
Message Authenticator Code Key	<input type="text"/>
Key Input Format	<input type="radio"/> ASCII <input checked="" type="radio"/> Hexadecimal

---

Authenticate Using

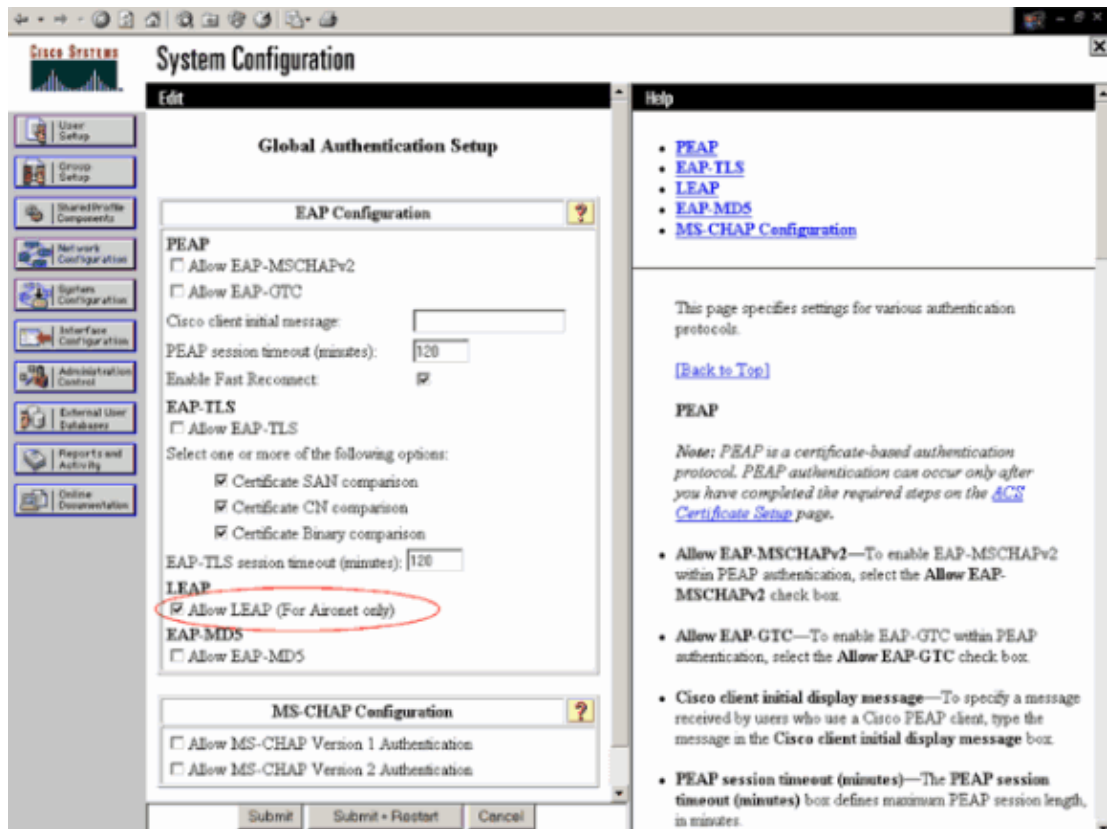
- ☐ Single Connect TACACS+ AAA Client (Record stop in accounting on failure)
- ☐ Log Update/Watchdog Packets from this AAA Client
- ☐ Log RADIUS Tunneling Packets from this AAA Client
- ☐ Replace RADIUS Port info with Username from this AAA Client
- ☐ Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

Submit

Submit + Apply

Cancel

4. Click **System Configuration** and **Global Authentication Setup** in order to ensure that the authentication server is configured to perform the desired EAP authentication method. Under the EAP configuration settings, choose the appropriate EAP method. This example uses LEAP authentication. Click **Submit** when you are done.

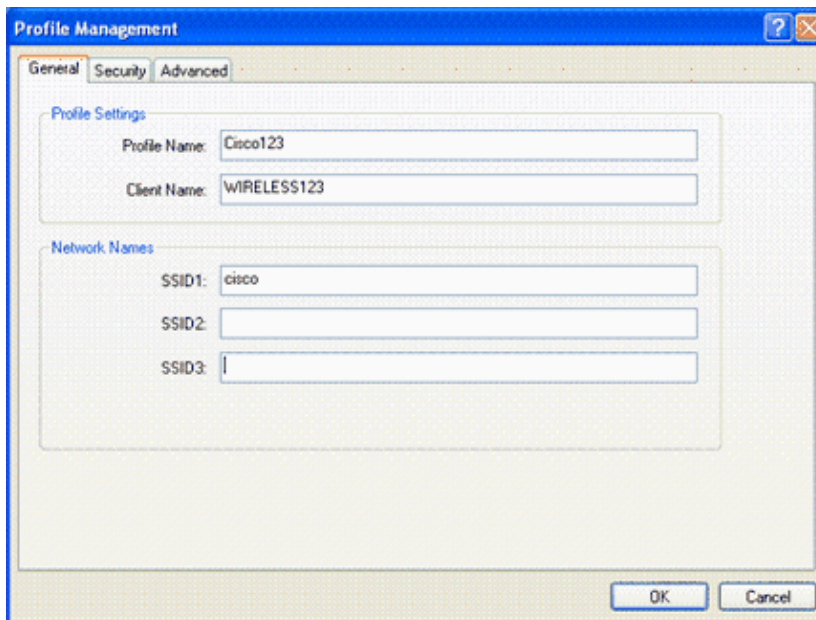


## Configure the Client

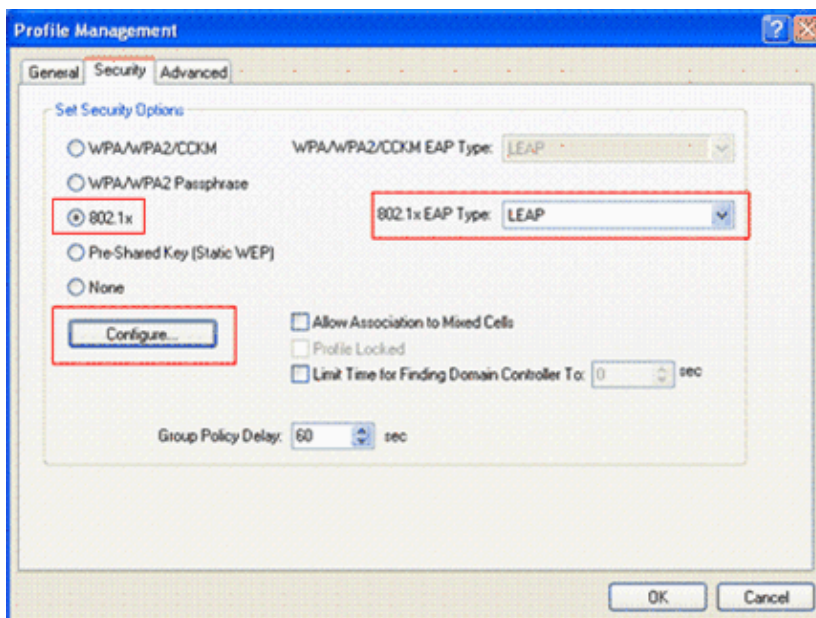
Client should also be configured for the appropriate EAP type. The client proposes the EAP type to the server during the EAP negotiation process. If the server supports that EAP type, it acknowledges the EAP type. If the EAP type is not supported, it sends a Negative acknowledgement and the client again negotiates with a different EAP method. This process continues until a supported EAP type is negotiated. This example uses LEAP as the EAP type.

Complete these steps in order to configure LEAP on the client with Aironet Desktop Utility .

1. Double-click on the **Aironet Utility** icon in order to open it.
2. Click the **Profile Management** tab.
3. Click on a profile and choose **Modify**.
4. Under the General tab, choose a *Profile Name*. Enter the **SSID** of the WLAN.



- Note:** SSID is case sensitive and it needs to exactly match with the SSID configured on the WLC.
5. Under the **Security** tab, choose *802.1x*. Choose the EAP type as **LEAP** and click **Configure**.

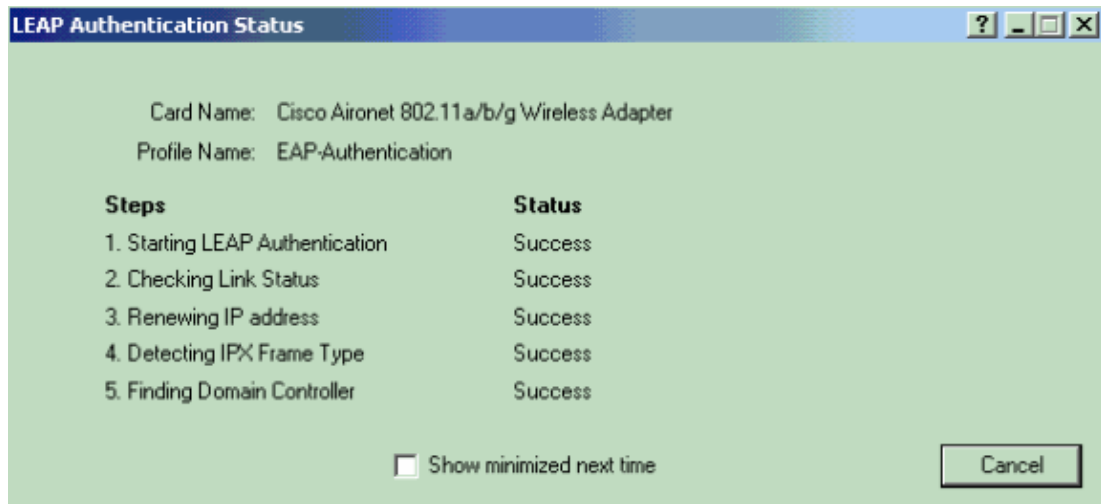


6. Choose **Use Temporary Username and Password**, which prompts you to enter the user credentials each time the computer reboots.

Check one of the three options given here. This example uses **Automatically Prompt for Username and Password**, which requires you to enter the *LEAP* user credentials in addition to the *Windows Username and Password* before you login to windows.

Check the **Always Resume the Secure Session** check box at the top of the window if you want the LEAP supplicant to always attempt to resume the previous session without the need to prompt you to re-enter your credentials whenever the client adapter roams and reassociates to the network.

**Note:** Refer to the Configuring the Client Adapter section of the document Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG and PI21AG) Installation and Configuration Guide for more information other options.



7. Under the **Advanced** tab, you can configure the Preamble, Aironet extension and other 802.11 options such as Power, Frequency and so forth.
8. Click **Ok**. The client now tries to associate with the configured parameters.

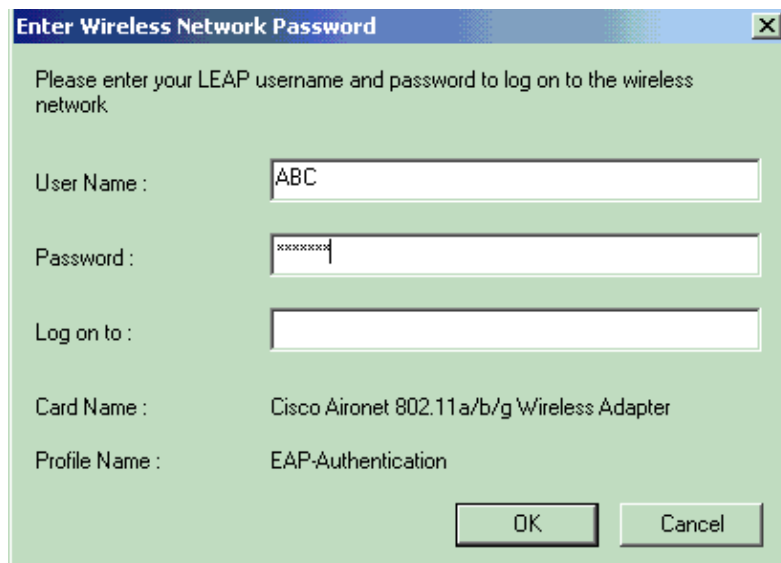
## Verify

Use this section to confirm that your configuration works properly.

Try to associate a wireless client with the Lightweight AP using LEAP authentication in order to verify if the configuration works as expected.

**Note:** This document assumes that the client profile is configured for LEAP authentication. Refer to Using EAP Authentication for more information on how to configure the 802.11 a/b/g Wireless Client Adapter for LEAP authentication.

Once the profile for the wireless client is activated, the user is asked to provide the username/password for LEAP authentication. Here is an example:



The Lightweight AP and then the WLC pass on the user credentials to the external RADIUS server (Cisco Secure ACS) in order to validate the credentials. The RADIUS server compares the data with the user database and provides access to the wireless client whenever the user credentials are valid in order to verify the user credentials. The Passed Authentication report on the ACS server shows that the client has passed the

RADIUS authentication. Here is an example:

The screenshot shows the Cisco Systems Reports and Activity page. On the left is a navigation menu with options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Database, Reports and Activity (selected), and Online Documentation. The main content area is titled 'Reports and Activity' and contains a 'Select' dropdown, a 'Refresh' button, and a 'Download' button. Below these is a table titled 'Passed Authentications active.csv'.

Date	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address
04/04/2006	15:01:33	Authen OK	ABC	Default Group	00-40-96-AC-E6-57	1	172.16.1.30
04/04/2006	15:00:37	Authen OK	ABC	Default Group	00-40-96-AC-E6-57	1	172.16.1.30

Upon successful RADIUS authentication the wireless client associates with the Lightweight AP.

The screenshot shows the 'LEAP Authentication Status' dialog box. It displays the card name 'Cisco Aironet 802.11a/b/g Wireless Adapter' and the profile name 'EAP-Authentication'. Below this is a table showing the steps of the authentication process and their status.

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	Success

At the bottom of the dialog, there is a checkbox labeled 'Show minimized next time' and a 'Cancel' button.

This can also be checked under the **Monitor** tab of WLC GUI. Choose **Monitor** > **Clients** and check for the MAC address of the client.

Save Configuration Ping Logout Refresh

MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Monitor

Summary

Statistics

Controller Ports

Wireless

Rogue APs

Known Rogue APs

Rogue Clients

Adhoc Routers

802.11a Radios

802.11b/g Radios

Clients

RADIUS Servers

Clients

Items 1 to 1 of 1

Search by MAC address  Search

Client MAC Addr	AP Name	AP MAC Addr	WLAN	Type	Status	Auth	Port	
00:40:95:a0e6:57	ap:5b:fb:d0	00:0b:85:5b:fb:d0	Cisco123	802.11a	Associated	Yes	1	<a href="#">Details</a> <a href="#">View Test Results</a> <a href="#">Remove</a>

## Troubleshoot

Complete these steps to troubleshoot the configurations:

1. Use the **debug lwapp events enable** command in order to check if the AP registers with the WLC.
2. Check if the RADIUS server receives and validates the authentication request from the wireless client. Check the NAS-IP- Address, date and time in order to verify if the WLC was able to reach the Radius server.

Check the Passed Authentications and Failed Attempts reports on the ACS server in order to accomplish this. These reports are available under Reports and Activities on the ACS server. Here is an example when the RADIUS server authentication fails:

Cisco Systems

Reports and Activity

Select

Refresh Download

Failed Attempts active.csv

Date	Time	Message Type	User Name	Group Name	Caller ID	Authn-Failure-Code	Authn-Failure-Code	Authn-Data	NAS-Port	NAS-IP-Address
04/04/2006	15:42:51	Authn failed	cde		00-40-96-AC-E6-57	CS user unknown			1	172.16.1.30

Back to Help

**Note:** Refer to Obtaining Version and AAA Debug Information for Cisco Secure ACS for Windows for information on how to troubleshoot and obtain debug information on Cisco Secure ACS.

3. You can also use these **debug** commands in order to troubleshoot AAA authentication:

♦ **debug aaa all enable** Configures the debug of all AAA messages.



◆ **debug dot1x packet enable** Enables the debug of all dot1x packets.

Here is a sample output from the **debug 802.1x aaa enable** command.

(Cisco Controller) >**debug dot1x aaa enable**

```
*Sep 23 15:15:43.792: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31) index=
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30) index=2
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32) index=5
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=11
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 AAA EAP Packet created request = 0x1533a288.
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2, length=8, id=
*Sep 23 15:15:43.794: 00000000: 02 02 00 08 01 41 42 43
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 [BE-req] Sending auth request to 'RADIUS' (g
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim Response'
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 AAA Message 'Interim Response' received for
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Received EAP Attribute (code=1, length=19,id
*Sep 23 15:15:43.799: 00000000: 01 03 00 13 11 01 00 08 42 3a 8e d1 18 24 e8 9f
*Sep 23 15:15:43.799: 00000010: 41 42 43
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile 00:40:96:ac:c
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31) index=
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30) index=2
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32) index=5
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 AAA EAP Packet created request = 0x1533a288.
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2, length=35, id
*Sep 23 15:15:43.902: 00000000: 02 03 00 23 11 01 00 18 83 f1 5b 32 cf 65 04 ed
*Sep 23 15:15:43.902: 00000010: da c8 4f 95 b4 2e 35 ac c0 6b bd fa 57 50 f3 13
*Sep 23 15:15:43.904: 00000020: 41 42 43
*Sep 23 15:15:43.904: 00:40:96:ac:dd:05 [BE-req] Sending auth request to 'RADIUS' (g
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim Response'
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 AAA Message 'Interim Response' received for
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Received EAP Attribute (code=3, length=4,id=
*Sep 23 15:15:43.907: 00000000: 03 03 00 04
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile 00:40:96:ac:c
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31) index=
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30) index=2
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32) index=5
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12
```



```

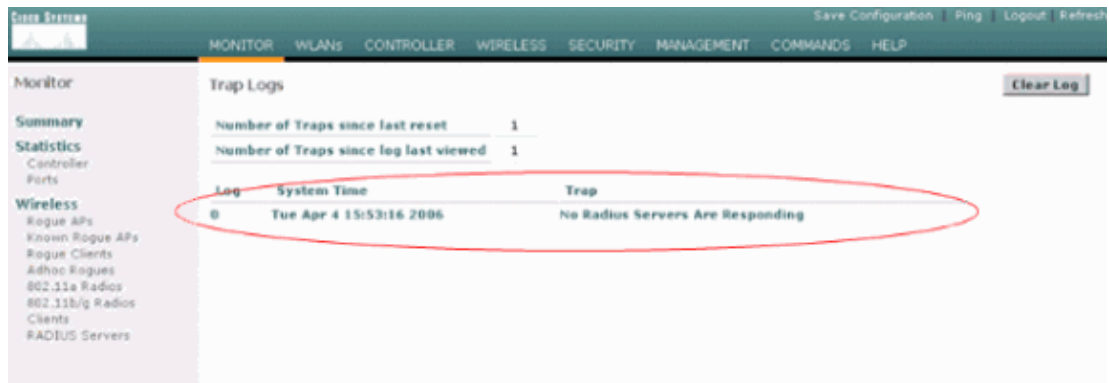
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 AAA EAP Packet created request = 0x1533a288.
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Sending EAP Attribute (code=1, length=19, id
*Sep 23 15:15:43.915: 00000000: 01 03 00 13 11 01 00 08 29 23 be 84 e1 6c d6 ae ..
*Sep 23 15:15:43.915: 00000010: 41 42 43
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 [BE-req] Sending auth request to 'RADIUS' (p
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Success'
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 AAA Message 'Success' received for mobile 00
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[0]: attribute 8, vendorId 0
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[1]: attribute 79, vendorId 0
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 Received EAP Attribute (code=2, length=35,id
*Sep 23 15:15:43.918: 00000000: 02 03 00 23 11 01 00 18 03 66 2c 6a b3 a6 c3 4c ..
*Sep 23 15:15:43.918: 00000010: 98 ac 69 f0 1b e8 8f a2 29 eb 56 d6 92 ce 60 a6 ..
*Sep 23 15:15:43.918: 00000020: 41 42 43
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[2]: attribute 1, vendorId 9
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[3]: attribute 25, vendorId 0
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[4]: attribute 80, vendorId 0

```

4. Monitor the logs on the WLC in order to check if the RADIUS server receives the user credentials. Click **Monitor** in order to check the logs from the WLC GUI. From the left-hand side menu, click **Statistics** and click **Radius server** from the list of options.

This is very important because in some cases, the RADIUS server never receives the user credentials if the RADIUS server configuration on the WLC is incorrect.

This is how the logs appear on the WLC if the RADIUS parameters are configured incorrectly:



You can use a combination of the **show wlan summary** command in order to recognize which of your WLANs employ RADIUS server authentication. Then you can view the **show client summary** command in order to see which MAC addresses (clients) are successfully authenticated on RADIUS WLANs. You can also correlate this with your Cisco Secure ACS passed attempts or failed attempts logs.

## Troubleshooting Tips

- Verify on the controller that RADIUS server is in active state, and not on standby or disabled.
- Use the **ping** command in order to check if the Radius server is reachable from the WLC.
- Check if the RADIUS server is selected from the drop down menu of the WLAN (SSID).
- If you use WPA, then you have to install the latest Microsoft WPA hotfix for Windows XP SP2. Also, you should upgrade the driver for your client supplicant to the latest.
- **DOT1X-1-MAX\_EAPOL\_KEY\_RETRANS\_FOR\_MOBILE: MAX\_EAPOL-Key M1 retransmissions reached for mobile xx:xx:xx:xx:xx**

This error message indicates that the client does not respond in time to the controller during the WPA (802.1x) key negotiation. The controllers set a timer for a response during key negotiation.

Typically when you see this message, it is due to an issue with the supplicant. Ensure that you run the latest versions of Client drivers and firmware. You can extend the EAP timers on the controllers to wait for client 802.1x info if you use these commands on the WLC CLI:

```
config advanced eap identity-request-timeout 120
config advanced eap identity-request-retries 20
config advanced eap request-timeout 120
config advanced eap request-retries 20
save config
```

- If you do PEAP, for example certificates with XP, SP2 where the cards are managed by the Microsoft wireless-0 utility, you need to get the KB885453 patch from Microsoft.

If you use Windows Zero Config/client supplicant, disable **Enable Fast Reconnect**. You can do this if you choose **Wireless Network Connection Properties > Wireless Networks > Preferred networks**. Then choose **SSID > Properties > Open > WEP > Authentication > EAP type > PEAP > Properties > Enable Fast Reconnect**. You can then find the option to enable or disable at the end of the window.

- If you have Intel 2200 or 2915 cards, refer to the statements on the Intel website about the known issues with their cards:

- ◆ Intel® PRO/Wireless 2200BG Network Connection
- ◆ Intel® PRO/Wireless 2915ABG Network Connection

Download the most current Intel drivers in order to avoid any issues. You can download Intel drivers at <http://downloadcenter.intel.com/>

- If the aggressive failover feature is enabled in WLC, the WLC is too aggressive to mark the AAA server as not responding. But, this should not be done because the AAA server is possibly not responsive only to that particular client, if you do silent discard. It can be a response to other valid clients with valid certificates. But, the WLC can still mark the AAA server as not responding and not functional.

In order to overcome this, disable the aggressive failover feature. Issue the **config radius aggressive-failover disable** command from the controller GUI in order to perform this. If this is disabled, then the controller only fails over to the next AAA server if there are three consecutive clients that fail to receive a response from the RADIUS server.

## Extracting the Package File from ACS RADIUS Server for Troubleshooting

If you use ACS as the external radius server, this section can be used to troubleshoot your configuration. The package.cab is a Zip file that contains all the necessary files needed in order to troubleshoot ACS efficiently. You can use the CSSupport.exe utility to create the package.cab, or you can collect the files manually.

Refer to the Creating a package.cab File section of *Obtaining Version and AAA Debug Information for Cisco Secure ACS for Windows* for more information on how to create and extract the package file from WCS.

---

## Related Information

- **WLAN Controller Failover for Lightweight Access Points Configuration Example**
  - **Wireless LAN Controller (WLC) Software Upgrade**
  - **Cisco Wireless LAN Controller Command Reference**
  - **Wireless Support Page**
  - **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Mar 03, 2009

Document ID: 69730

---