Wi−Fi Protected Access 2 (WPA 2) Configuration Example

Document ID: 67134

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Background Information
WPA 2 Support with Cisco Aironet Equipment
Configure in Enterprise Mode
Network Setup
Configure the AP
CLI Configuration
Configure the Client Adapter
Verify
Troubleshoot
Configure in Personal Mode
Network Setup
Configure the AP
Configure the Client Adapter
Verify
Troubleshoot
Related Information

Introduction

This document explains the advantages of the use of Wi−Fi Protected Access 2 (WPA 2) in a Wireless LAN (WLAN). The document provides two configuration examples on how to implement WPA 2 on a WLAN. The first example shows how to configure WPA 2 in enterprise mode, and the second example configures WPA 2 in personal mode.

Note: WPA works with Extensible Authentication Protocol (EAP).

Prerequisites

Requirements

Ensure that you have basic knowledge of these topics before you attempt this configuration:

- WPA
- WLAN security solutions

Note: Refer to Cisco Aironet Wireless LAN Security Overview for information on Cisco WLAN security solutions.

Components Used

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

- Cisco Aironet 1310G Access Point (AP)/Bridge that runs Cisco IOS® Software Release 12.3(2)JA
- Aironet 802.11a/b/g CB21AG Client Adapter that runs firmware 2.5
- Aironet Desktop Utility (ADU) that runs firmware 2.5

Note: The Aironet CB21AG and PI21AG client adapter software is incompatible with other Aironet client adapter software. You must use the ADU with CB21AG and PI21AG cards, and you must use the Aironet Client Utility (ACU) all other Aironet client adapters. Refer to Installing the Client Adapter for more information on how to install the CB21AG card and ADU.

Note: This document uses an AP/bridge that has an integrated antenna. If you use an AP/bridge which requires an external antenna, ensure that the antennas are connected to the AP/bridge. Otherwise, the AP/bridge is unable to connect to the wireless network. Certain AP/bridge models come with integrated antennas, whereas others need an external antenna for general operation. For information on the AP/bridge models that come with internal or external antennas, refer to the ordering guide/product guide of the appropriate device.

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.

Background Information

WPA is a standard−based security solution from the Wi−Fi Alliance that addresses the vulnerabilities in native WLANs. WPA provides enhanced data protection and access control for WLAN systems. WPA addresses all known Wired Equivalent Privacy (WEP) vulnerabilities in the original IEEE 802.11 security implementation and brings an immediate security solution to WLANs in both enterprise and small office, home office (SOHO) environments.

WPA 2 is the next generation of Wi−Fi security. WPA 2 is the Wi−Fi Alliance interoperable implementation of the ratified IEEE 802.11i standard. WPA 2 implements the National Institute of Standards and Technology (NIST)−recommended Advanced Encryption Standard (AES) encryption algorithm with the use of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). AES Counter Mode is a block cipher that encrypts 128−bit blocks of data at a time with a 128−bit encryption key. The CCMP algorithm produces a message integrity code (MIC) that provides data origin authentication and data integrity for the wireless frame.

Note: CCMP is also referred to as CBC−MAC.

WPA 2 offers a higher level of security than WPA because AES offers stronger encryption than Temporal Key Integrity Protocol (TKIP). TKIP is the encryption algorithm that WPA uses. WPA 2 creates fresh session keys on every association. The encryption keys that are used for each client on the network are unique and specific to that client. Ultimately, every packet that is sent over the air is encrypted with a unique key. Security is enhanced with the use of a new and unique encryption key because there is no key reuse. WPA is still considered secure and TKIP has not been broken. However, Cisco recommends that customers transition to WPA 2 as soon as possible.

WPA and WPA 2 both support two modes of operation:

- Enterprise mode
- Personal mode

This document discusses the implementation of these two modes with WPA 2.

WPA 2 Support with Cisco Aironet Equipment

WPA 2 is supported on this equipment:

- Aironet 1130AG AP series and 1230AG AP series
- Aironet 1100 AP series
- Aironet 1200 AP series
- Aironet 1300 AP series

Note: Equip these APs with 802.11g radios and use Cisco IOS Software Release 12.3(2)JA or later.

WPA 2 and AES are also supported on:

- Aironet 1200 series radio modules with the part numbers AIR−RM21A and AIR−RM22A

  Note: The Aironet 1200 radio module with the part number AIR−RM20A does not support WPA 2.
- Aironet 802.11a/b/g Client Adapters with firmware version 2.5

Note: Cisco Aironet 350 series products do not support WPA 2 because their radios lack AES support.

Note: Cisco Aironet 1400 Series Wireless Bridges do not support WPA 2 or AES.

Configure in Enterprise Mode

The term **enterprise mode** refers to products that are tested to be interoperable in both Pre−Shared Key (PSK) and IEEE 802.1x modes of operation for authentication. The 802.1x is considered to be more secure than any of the legacy authentication frameworks because of its flexibility in support of a variety of authentication mechanisms and stronger encryption algorithms. WPA 2 in enterprise mode performs authentication in two phases. Configuration of open authentication occurs in the first phase. The second phase is 802.1x authentication with one of the EAP methods. AES provides the encryption mechanism.

In enterprise mode, clients and authentication servers authenticate each other with the use of an EAP authentication method, and the client and server generate a Pairwise Master Key (PMK). With WPA 2, the server generates the PMK dynamically and passes the PMK to the AP.

This section discusses the configuration that is necessary to implement WPA 2 in the enterprise mode of operation.

Network Setup

In this setup, an Aironet 1310G AP/Bridge that runs Cisco Lightweight Extensible Authentication Protocol (LEAP) authenticates a user with a WPA 2−compatible client adapter. Key management occurs with the use of WPA 2, on which AES−CCMP encryption is configured. The AP is configured as a local RADIUS server that runs LEAP authentication. You must configure the client adapter and the AP in order to implement this setup. The sections Configure the AP and Configure the Client Adapter show the configuration on the AP and the client adapter.

Configure the AP

Complete these steps to configure the AP using GUI:

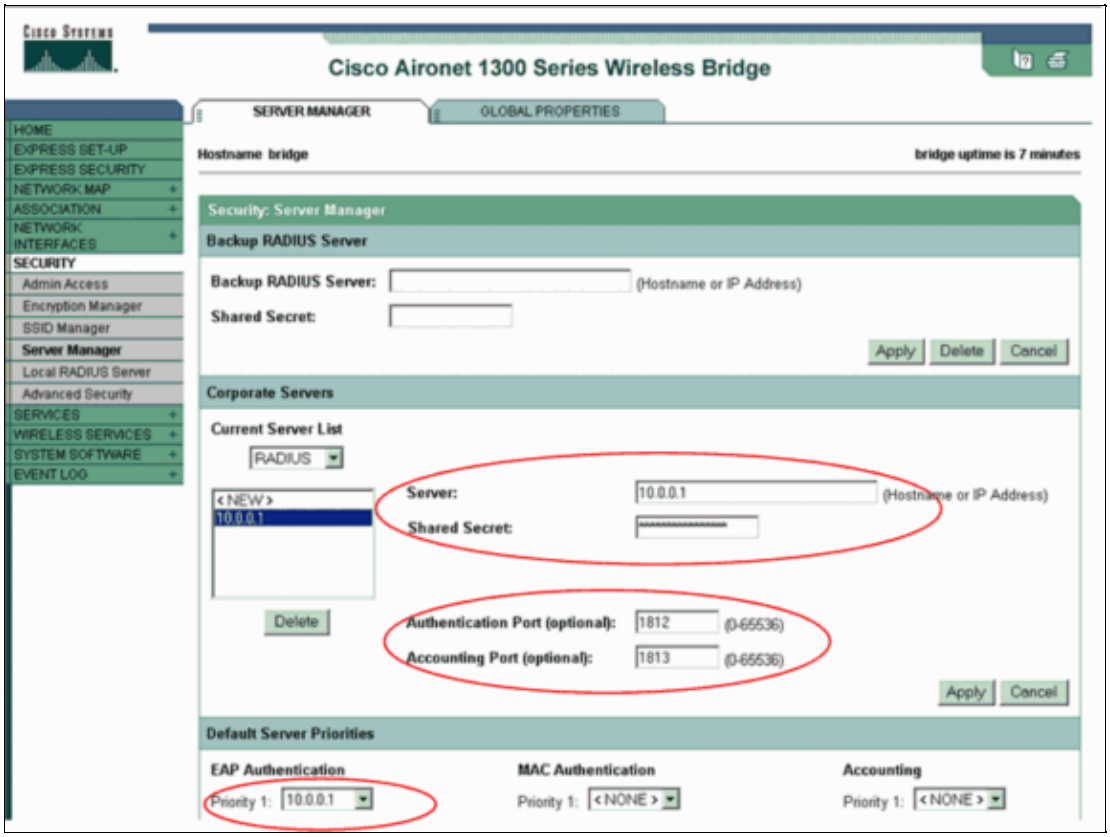
1. Configure the AP as a local RADIUS server that runs LEAP authentication.

    a. Choose **Security > Server Manager** in the menu on the left and define the IP address, ports, and shared secret of the RADIUS server.

    Because this configuration configures the AP as a local RADIUS server, use the IP address of the AP. Use the ports 1812 and 1813 for local RADIUS server operation.

    b. In the Default Server Priorities area, define the default EAP authentication priority as 10.0.0.1.

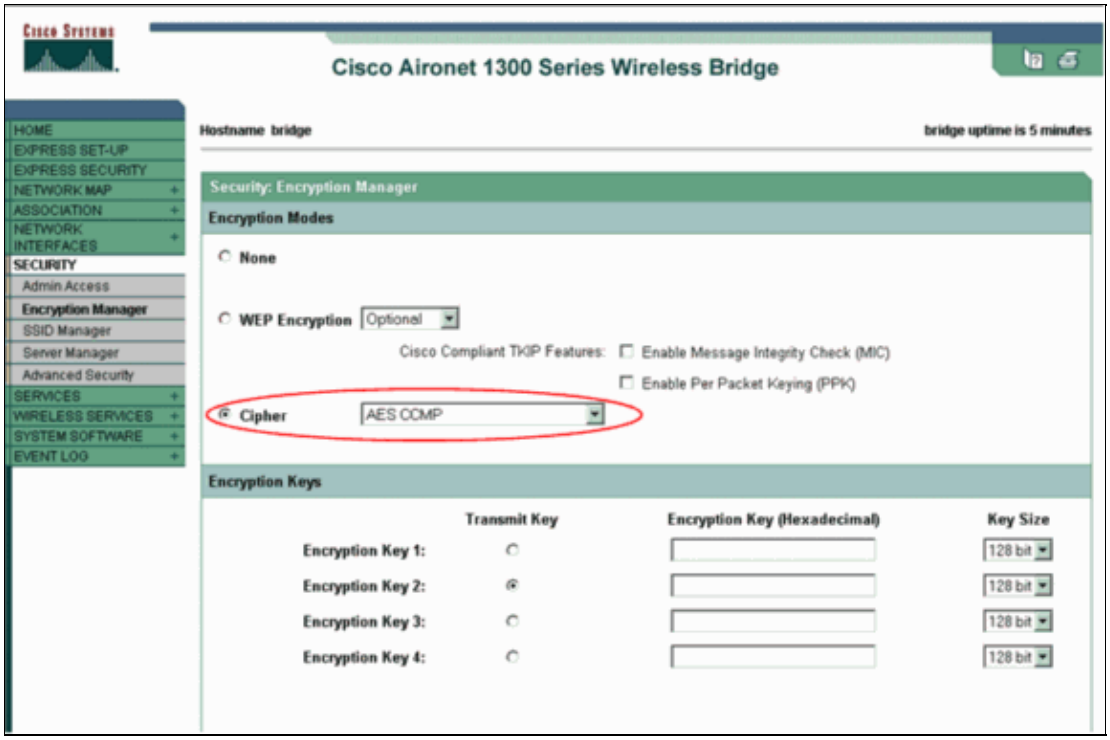
    Note: 10.0.0.1 is the local RADIUS server.



2. Choose **Security > Encryption Manager** from the menu on the left and complete these steps:

    a. From the Cipher menu, choose **AES CCMP**.

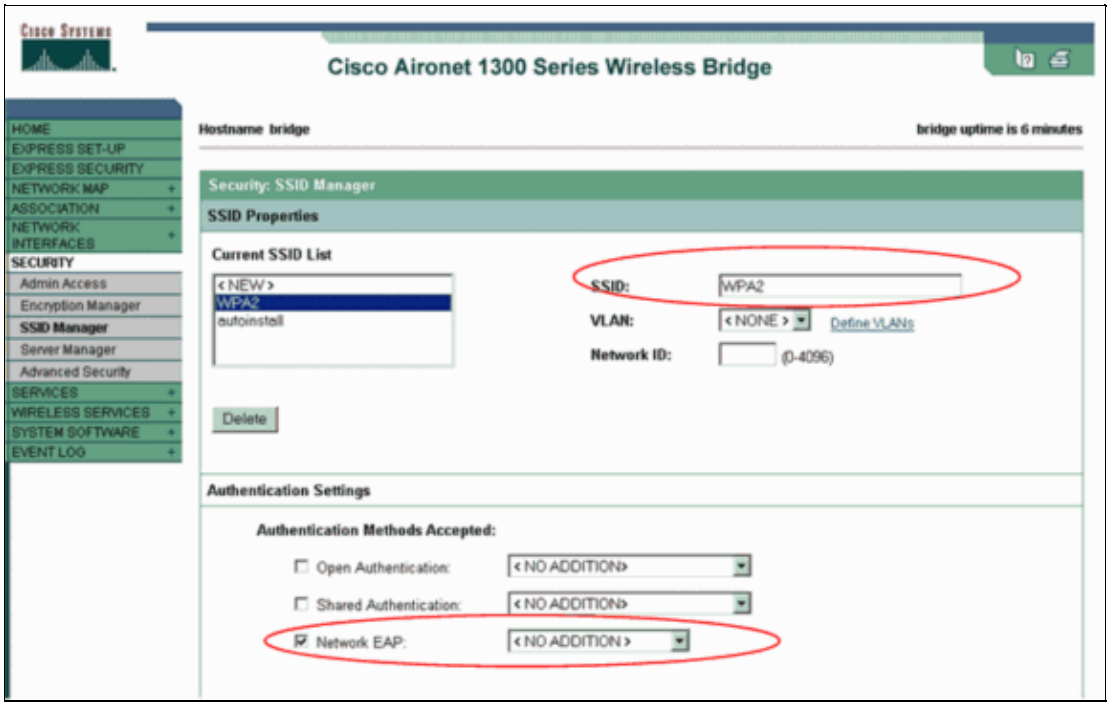
    This option enables AES encryption with the use of Counter Mode with CBC−MAC.



b. Click **Apply**.

3. Choose **Security > SSID Manager** and create a new Service Set Identifier (SSID) for use with WPA 2.

a. Check the **Network EAP** check box in the Authentication Methods Accepted area.



Note: Use these guidelines when you configure the authentication type on the radio interface:

◊ Cisco clients Use Network EAP.
◊ Third−party clients (which include Cisco Compatible Extensions [CCX]−compliant products) Use Open Authentication with EAP.
◊ A combination of both Cisco and third−party clients Choose both Network EAP and

Open Authentication with EAP.

b. Scroll down the Security SSID Manager window to the Authenticated Key Management area and complete these steps:

   a. From the Key Management menu, choose **Mandatory**.
   b. Check the **WPA** check box on the right.

c. Click **Apply**.

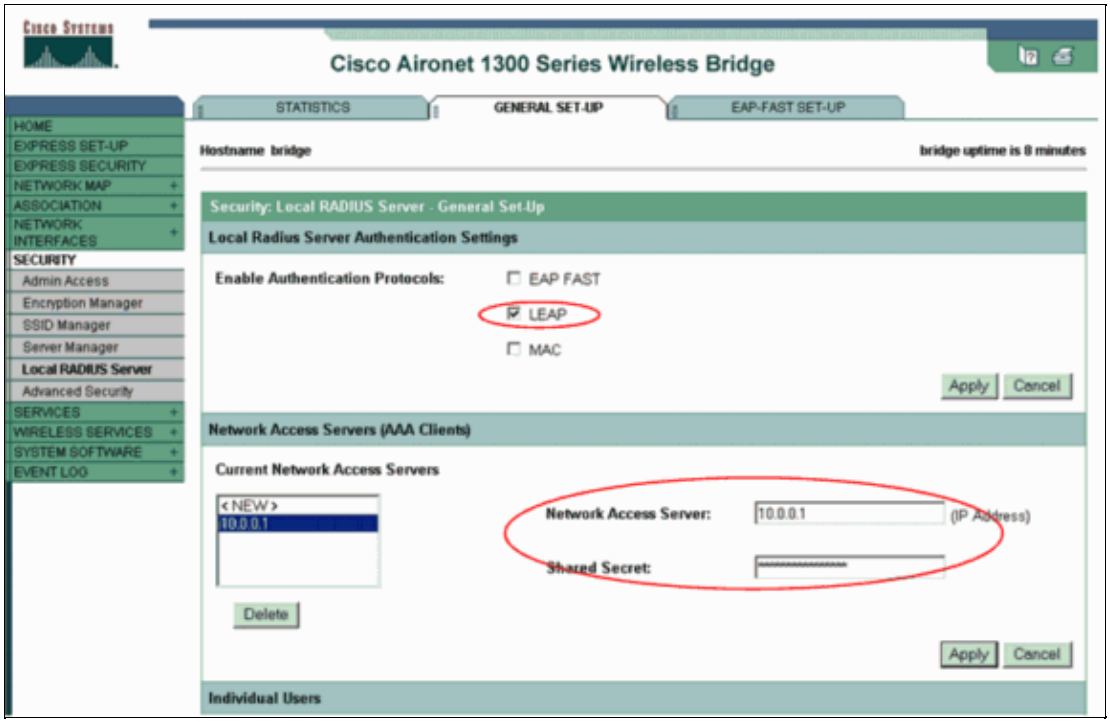
Note: The definition of VLANs is optional. If you define VLANs, client devices that associate with use of this SSID are grouped into the VLAN. Refer to Configuring VLANs for more information on how to implement VLANs.



4. Choose **Security > Local Radius Server** and complete these steps:

   a. Click the **General Set−Up** tab located at the top of the window.
   b. Check the **LEAP** check box and click **Apply**.
   c. In the Network Access Servers area, define the IP address and shared secret of the RADIUS server.

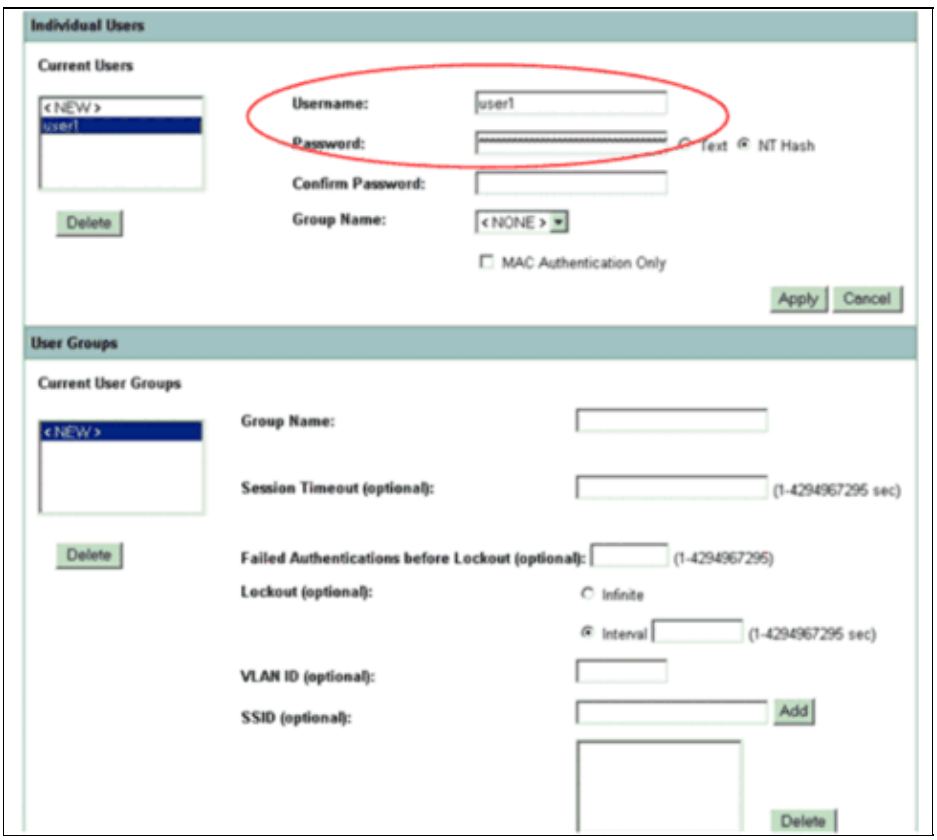
      For the local RADIUS server, use the IP address of the AP.



d. Click **Apply**.

5. Scroll down the General Set−Up window to the Individual Users area and define the individual users.

   The definition of the user groups is optional.



This configuration defines a user with the name "user1" and a password. Also, the configuration selects NT hash for the password. After completion of the procedure in this section, the AP is ready to accept authentication requests from clients. The next step is to configure the client adapter.

CLI Configuration

Access Point

```
ap#show running-config
Building configuration...
.
.
.
aaa new-model

!--- This command reinitializes the authentication,
!--- authorization and accounting functions.

!
!
aaa group server radius rad_eap
 server 10.0.0.1 auth-port 1812 acct-port 1813

!--- A server group for RADIUS is created called "rad_eap"
!--- that uses the server at 10.0.0.1 on ports 1812 and 1813.

.
.
.
aaa authentication login eap_methods group rad_eap

!--- Authentication [user validation] is to be done for
!--- users in a group called "eap_methods" who use server group "rad_eap".

.
.
.
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 1 key 1 size 128bit
   12345678901234567890123456 transmit-key

!---This step is optional
!--- This value seeds the initial key for use with
!--- broadcast [255.255.255.255] traffic.  If more than one VLAN is
!--- used, then keys must be set for each VLAN.

 encryption vlan 1 mode wep mandatory

!--- This defines the policy for the use of Wired Equivalent Privacy (WEP).
!--- If more than one VLAN is used,
!--- the policy must be set to mandatory for each VLAN.

 broadcast-key vlan 1 change 300

!--- You can also enable Broadcast Key Rotation for each vlan and Specify the time
   after which Brodacst key is changed. If it is disabled Broadcast Key is still
   used but not changed.

ssid cisco vlan 1

!--- Create a SSID Assign a vlan to this SSID

 authentication open eap eap_methods
```

```
 authentication network-eap eap_methods

!--- Expect that users who attach to SSID "cisco"
!--- request authentication with the type 128 Open EAP and Network EAP  authentication
!--- bit set in the headers of those requests, and group those users into
!--- a group called "eap_methods."

 !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
 channel 2437
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
.
.
.
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 10.0.0.1 255.255.255.0

!--- The address of this unit.

 no ip route-cache
!
ip default-gateway 10.77.244.194
ip http server
ip http help-path
   http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100
ip radius source-interface BVI1
snmp-server community cable RO
snmp-server enable traps tty
radius-server local

!--- Engages the Local RADIUS Server feature.

  nas 10.0.0.1 key shared_secret

!--- Identifies itself as a RADIUS server, reiterates
!--- "localness" and defines the key between the server (itself) and the access point(itself).

  !
  group testuser

!--- Groups are optional.

  !
  user user1 nthash password1 group testuser

!--- Individual user

  user user2 nthash password2 group testuser

!--- Individual user
```

```
!--- These individual users comprise the Local Database

!
radius-server host 10.0.0.1 auth-port 1812 acct-port
   1813 key shared_secret

!--- Defines where the RADIUS server is and the key between
!--- the access point (itself) and the server.

radius-server retransmit 3
radius-server attribute 32 include-in-access-req format %h
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
bridge 1 route ip
!
!
line con 0
line vty 5 15
!
end
```

Configure the Client Adapter

Complete these steps:

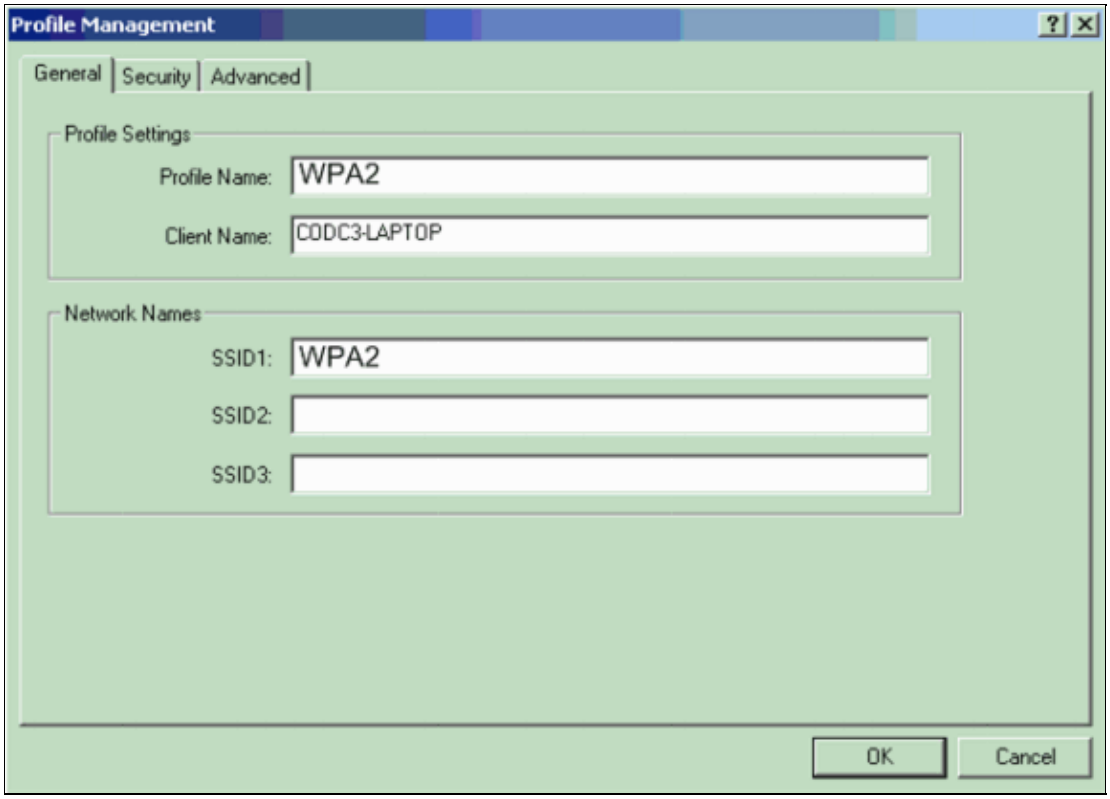
Note: This document uses an Aironet 802.11a/b/g Client Adapter that runs firmware 2.5 and explains the configuration of the client adapter with ADU version 2.5.

1. In the Profile Management window on the ADU, click **New** in order to create a new profile.

   A new window displays where you can set the configuration for WPA 2 enterprise mode operation. Under the General tab, enter the Profile Name and the SSID that the client adapter will use.

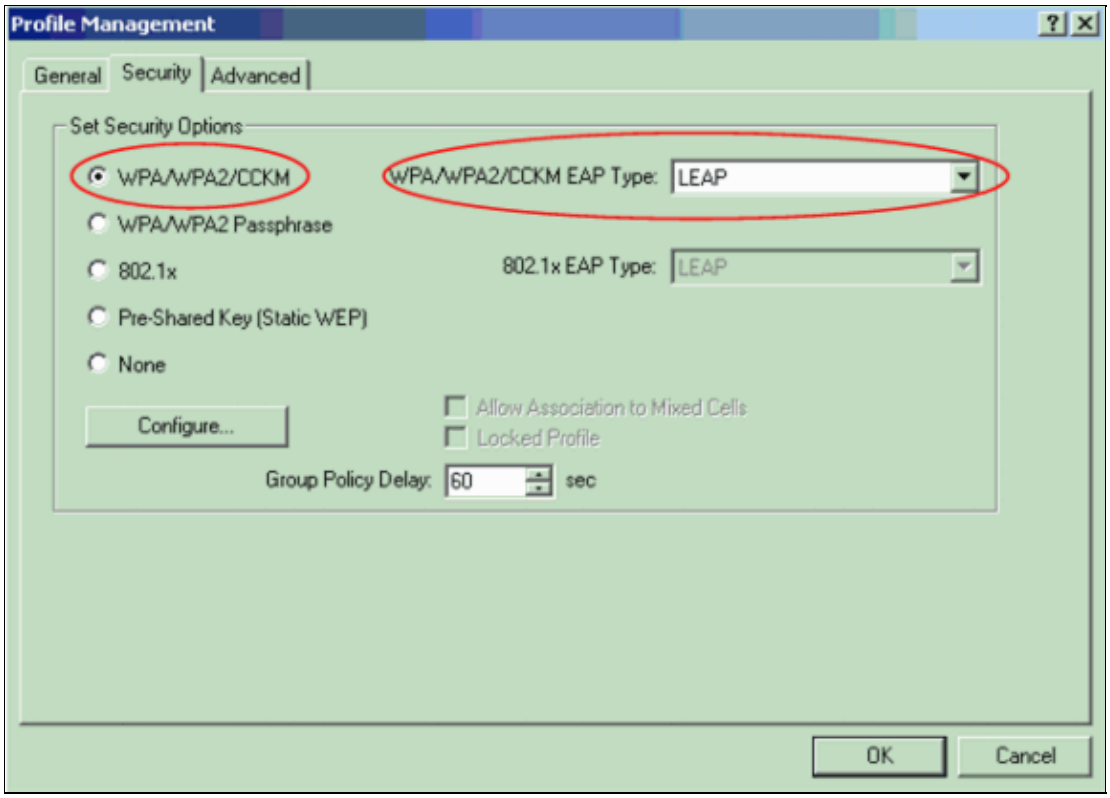
   In this example, the profile name and the SSID are WPA2:

   Note: The SSID must match the SSID that you configured on the AP for WPA 2.



2. Click the **Security** tab, click **WPA/WPA2/CCKM**, and choose **LEAP** from the WPA/WPA2/CCKM EAP Type menu.

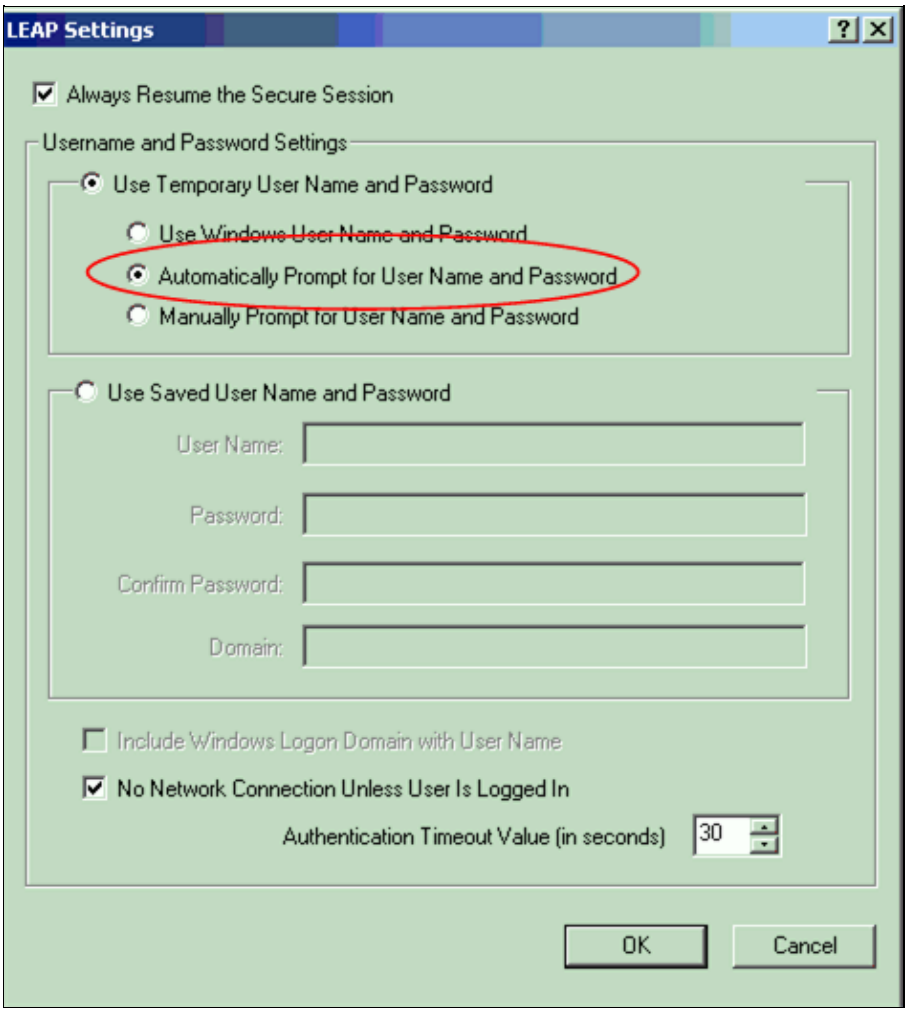
   This action enables either WPA or WPA 2, whichever you configure on the AP.



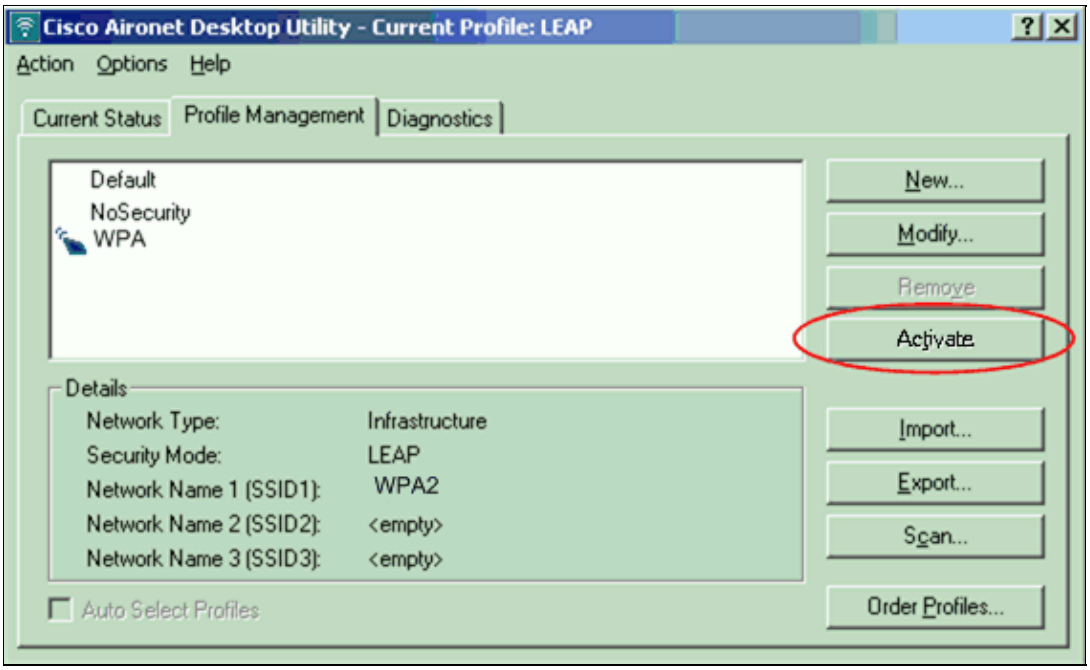
3. Click **Configure** in order to define LEAP settings.
4. Choose the appropriate Username and Password Settings, based on the requirements, and click **OK**.

   This configuration chooses the option Automatically Prompt for User Name and Password. This

option enables you to manually enter the user name and password when LEAP authentication takes place.



5. Click **OK** in order to exit the Profile Management window.
6. Click **Activate** in order to enable this profile on the client adapter.



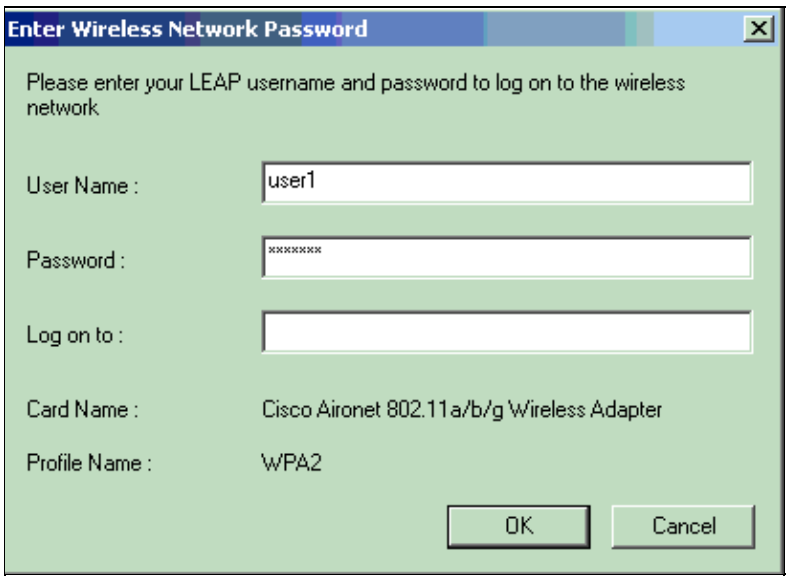
Note: If you use Microsoft Wireless Zero Configuration (WZC) to configure the client adapter, by default, WPA 2 is not available with WZC. So, in order to allow WZC−enabled clients to run WPA 2, you must install a hot fix for Microsoft Windows XP. Refer to the Microsoft Download Center − Update for Windows XP (KB893357) for the installation.

After you install the hot fix, you can configure WPA 2 with WZC.

Verify

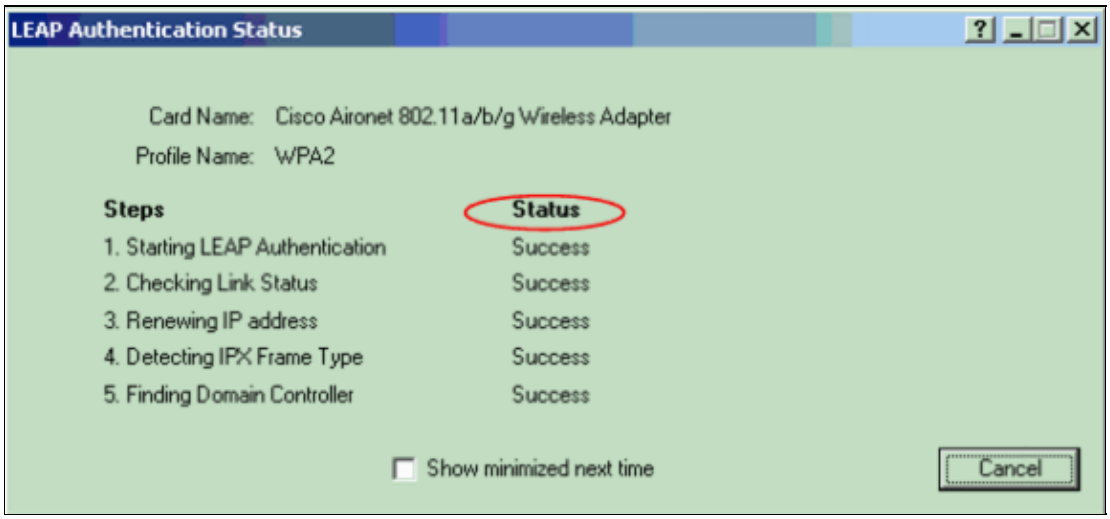
Use this section to confirm that your configuration works properly.

1. When the Enter Wireless Network Password window displays, enter the user name and password.



The next window is LEAP Authentication Status. This phase verifies the user credentials against the local RADIUS server.

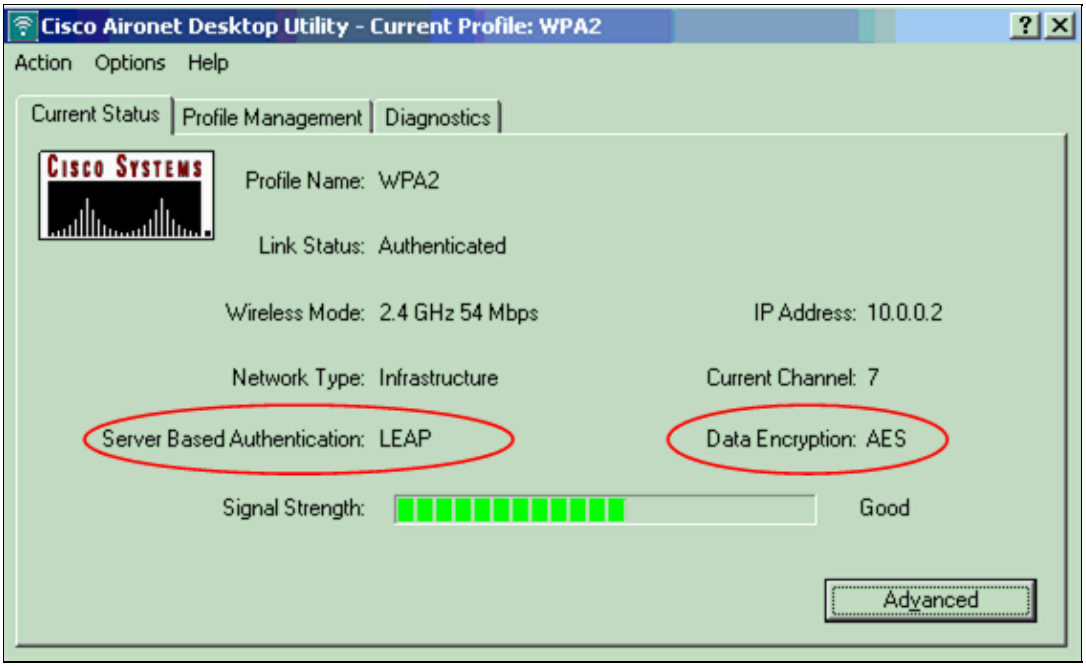
2. Check the Status area in order to see the result of the authentication.



When authentication is successful, the client connects to the wireless LAN.

3. Check the ADU Current Status in order to verify that the client uses AES encryption and LEAP authentication.

This shows that you have implemented WPA 2 with LEAP authentication and AES encryption in the WLAN.



4. Check the AP/bridge Event Log in order to verify that the client has been authenticated successfully with WPA 2.



Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Configure in Personal Mode

The term **personal mode** refers to products that are tested to be interoperable in the PSK−only mode of operation for authentication. This mode requires manual configuration of a PSK on the AP and clients. PSK authenticates users via a password, or identification code, on both the client station and the AP. No authentication server is necessary. A client can gain access to the network only if the client password matches the AP password. The password also provides the keying material that TKIP or AES uses to generate an

encryption key for the encryption of the data packets. Personal mode is targeted to SOHO environments and is not considered secure for enterprise environments. This section provides the configuration that you need to implement WPA 2 in the personal mode of operation.

Network Setup

In this setup, a user with a WPA 2−compatible client adapter authenticates to an Aironet 1310G AP/Bridge. Key management occurs with the use of WPA 2 PSK, with AES−CCMP encryption configured. The sections Configure the AP and Configure the Client Adapter show the configuration on the AP and the client adapter.

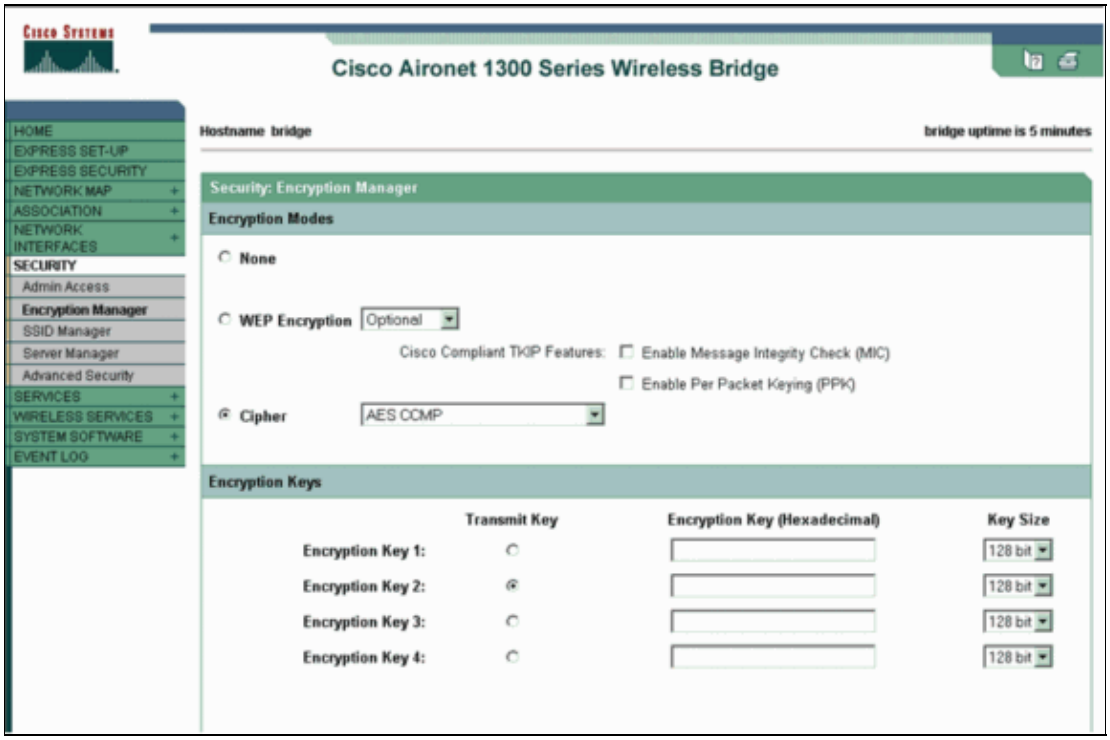
Configure the AP

Complete these steps:

1. Choose **Security > Encryption Manager** in the menu on the left and complete these steps:

    a. From the Cipher menu, choose **AES CCMP**.

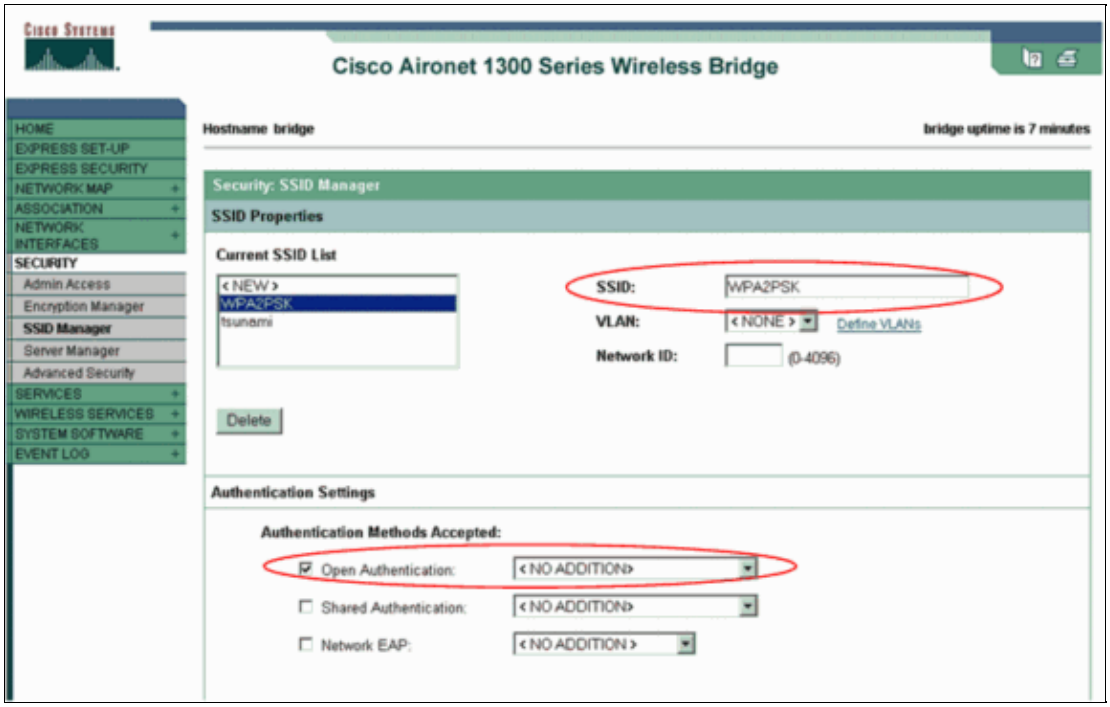
    This option enables AES encryption with the use of Counter Mode with CCMP.



    b. Click **Apply**.

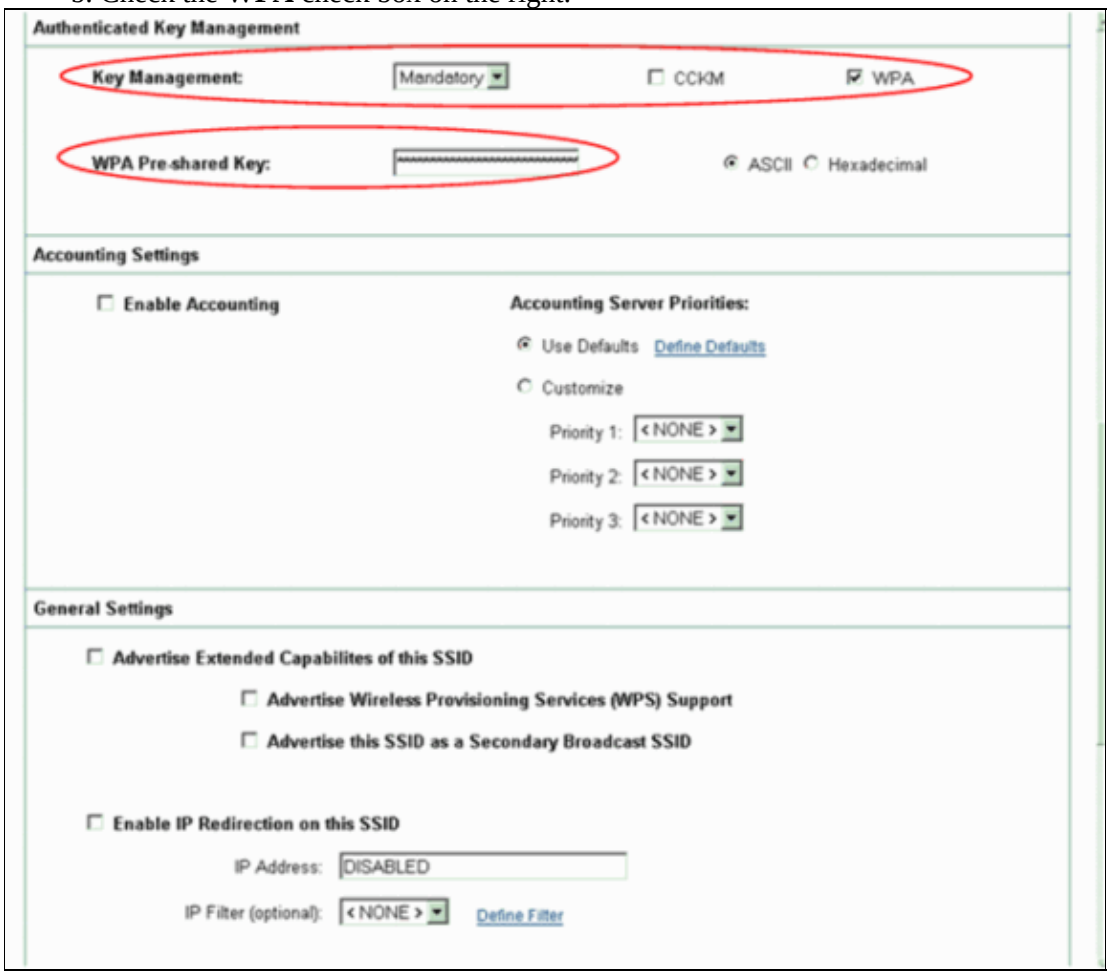
2. Choose **Security > SSID Manager** and create a new SSID for use with WPA 2.

    a. Check the **Open Authentication** check box.



b. Scroll down the Security: SSID Manager window to the Authenticated Key Management area and complete these steps:

   a. From the Key Management menu, choose **Mandatory**.
   b. Check the **WPA** check box on the right.



c. Enter the WPA PSK shared secret key or the WPA PSK passphrase key.

This key must match the WPA PSK key that you configure on the client adapter.

d. Click **Apply**.

The AP can now receive authentication requests from the wireless clients.

Configure the Client Adapter

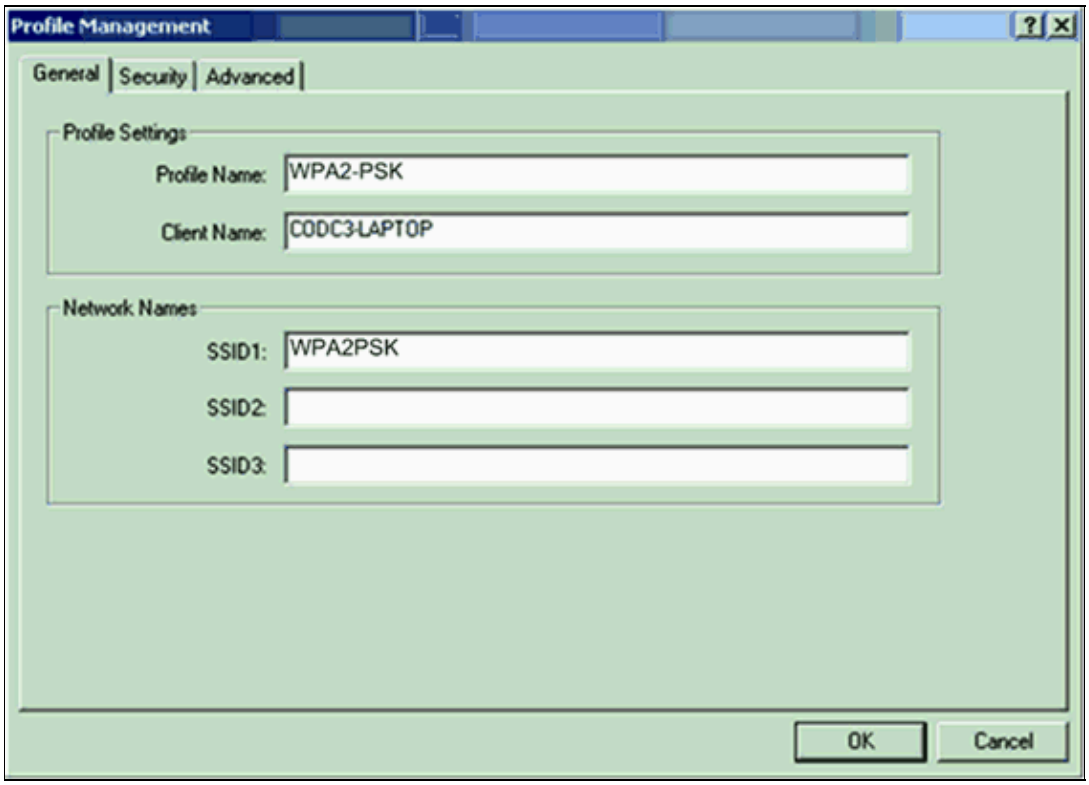
Complete these steps:

1. In the Profile Management window on the ADU, click **New** in order to create a new profile.

   A new window displays where you can set the configuration for WPA 2 PSK mode of operation. Under the General tab, enter the Profile Name and the SSID that the client adapter will use.

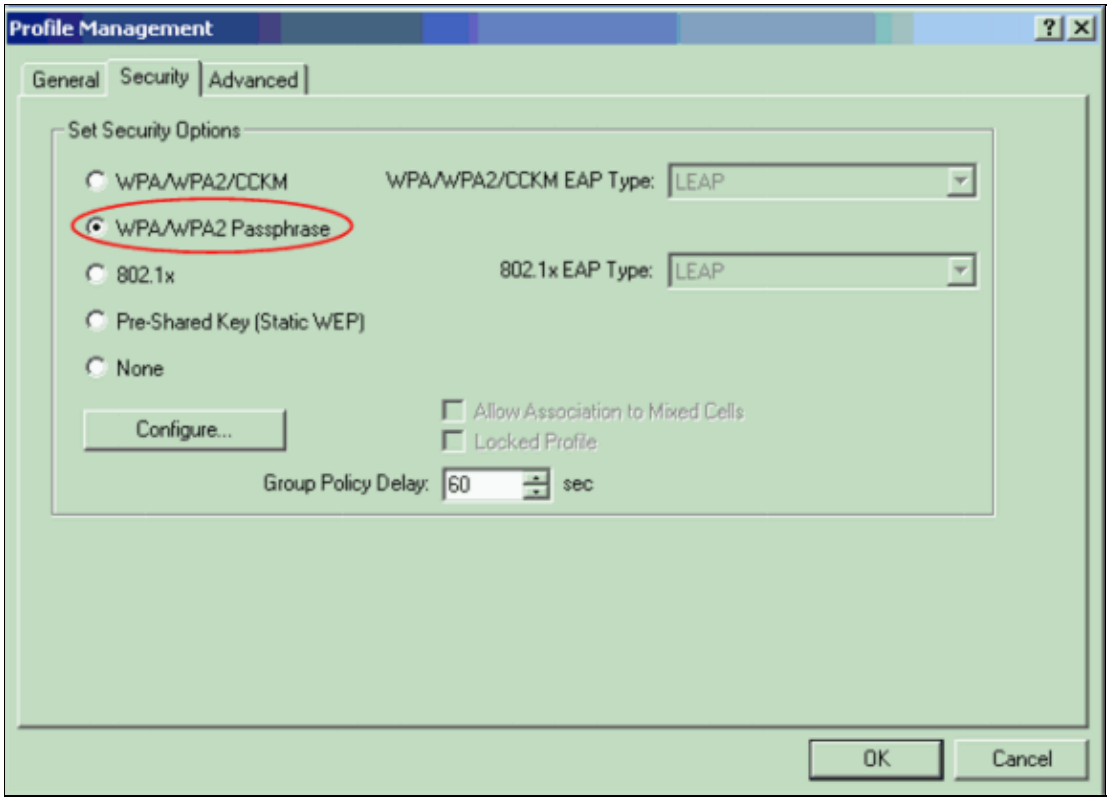
   In this example, the profile name is WPA2−PSK and the SSID is WPA2PSK:

   Note: The SSID must match the SSID that you configured on the AP for WPA 2 PSK.



2. Click the **Security** tab and click **WPA/WPA2 Passphrase**.

   This action enables either WPA PSK or WPA 2 PSK, whichever you configure on the AP.



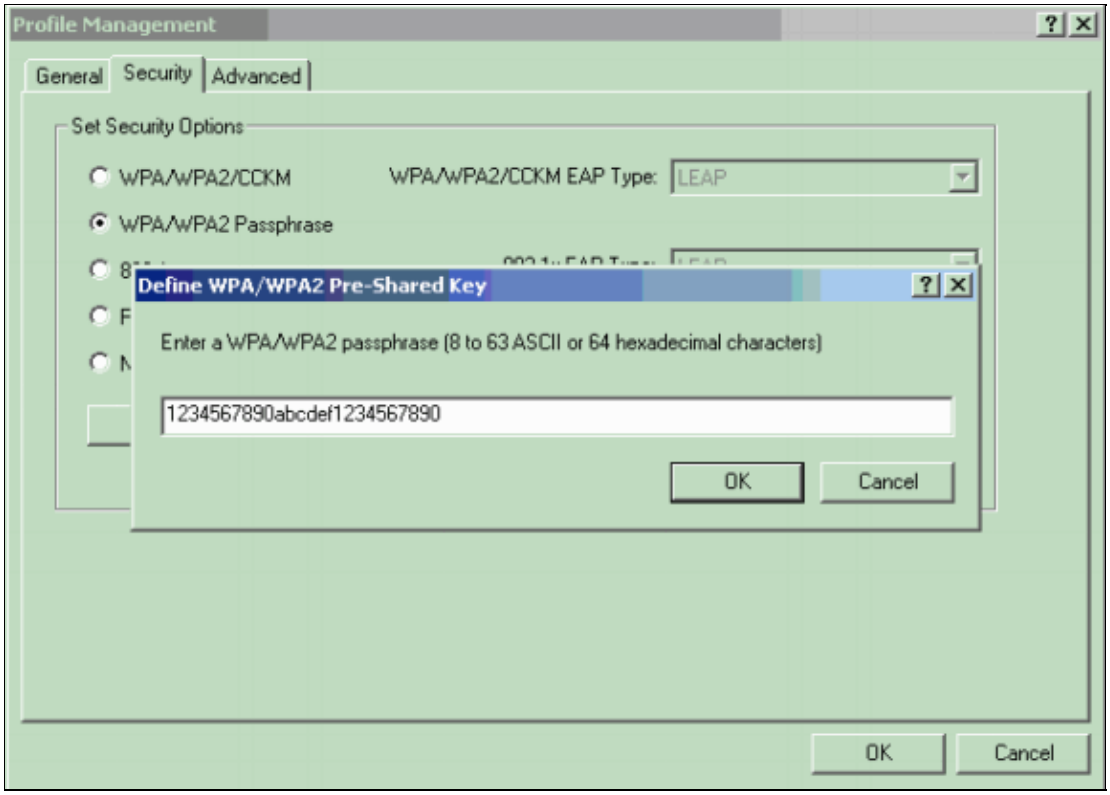
3. Click **Configure**.

   The Define WPA/WPA2 Pre−Shared Key window displays.
4. Obtain the WPA/WPA2 passphrase from your system administrator and enter the passphrase in the WPA/WPA2 passphrase field.

   Obtain the passphrase for the AP in an infrastructure network or the passphrase for other clients in an ad hoc network.

   Use these guidelines in order to enter a passphrase:

   - WPA/WPA2 passphrases must contain between 8 and 63 ASCII text characters or 64 hexadecimal characters.
   - Your client adapter WPA/WPA2 passphrase must match the passphrase of the AP with which you plan to communicate.



5. Click **OK** in order to save the passphrase and return to the Profile Management window.

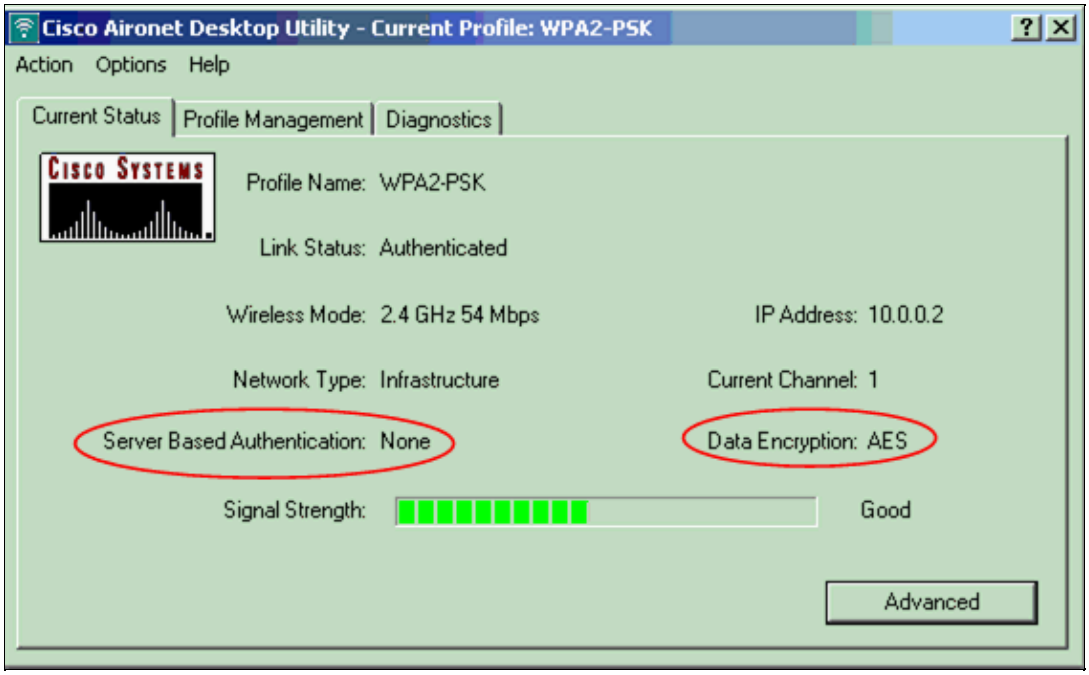
Verify

Use this section to confirm that your configuration works properly.

After the WPA 2 PSK profile is activated, the AP authenticates the client based on the WPA 2 passphrase (PSK) and provides access to the WLAN.

1. Check the ADU Current Status in order to verify successful authentication.

   This window provides an example. The window shows that the encryption that is used is AES and that no server−based authentication is performed:



2. Check the AP/bridge Event Log in order to verify that the client has been authenticated successfully with WPA 2 PSK mode of authentication.



Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Configuring Cipher Suites and WEP**
- **Configuring Authentication Types**
- **WPA Configuration Overview**
- **WPA2 − Wi−Fi Protected Access 2**
- **What is WPA mixed mode operation, and how do I configure it in my AP**
- **Wireless Support Page**
- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map
© 2014 − 2015 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Jan 21, 2008 Document ID: 67134