Wireless Authentication Types on a Fixed ISR Configuration Example

Document ID: 98499

Contents

Introduction

This document provides configuration example that explains how to configure various Layer 2 authentication types on a Cisco Wireless integrated fixed−configuration router for Wireless connectivity with CLI

commands.

Prerequisites

Requirements

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

- Knowledge of how to configure the basic parameters of the Cisco Integrated Services Router (ISR)
- Knowledge of how to configure the 802.11a/b/g Wireless Client Adapter with the Aironet Desktop Utility (ADU)

Components Used

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

- Cisco 877W ISR that runs Cisco IOS® Software Release 12.3(8)YI1
- Laptop with Aironet Desktop Utility Version 3.6
- 802.11 a/b/g Client Adapter that runs Firmware Version 3.6

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

Conventions

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

Background Information

The Cisco integrated services fixed−configuration routers support a secure, affordable, and easy−to−use wireless LAN solution that combines mobility and flexibility with the enterprise−class features required by networking professionals. With a management system based on Cisco IOS software, the Cisco routers act as access points and are Wi−Fi certified, IEEE 802.11a/b/g−compliant wireless LAN transceivers.

You can configure and monitor the routers with the command−line interface (CLI), the browser−based management system, or Simple Network Management Protocol (SNMP). This document describes how to configure the ISR for wireless connectivity with the CLI commands.

Configure

This example shows how to configure these authentication types on a Cisco Wireless Integrated fixed configuration router with CLI commands.

- Open authentication
- 802.1x/EAP (Extensible Authentication Protocol) authentication
- Wi−Fi Protected Access Pre−Shared Key (WPA−PSK) Authentication
- WPA (with EAP) authentication

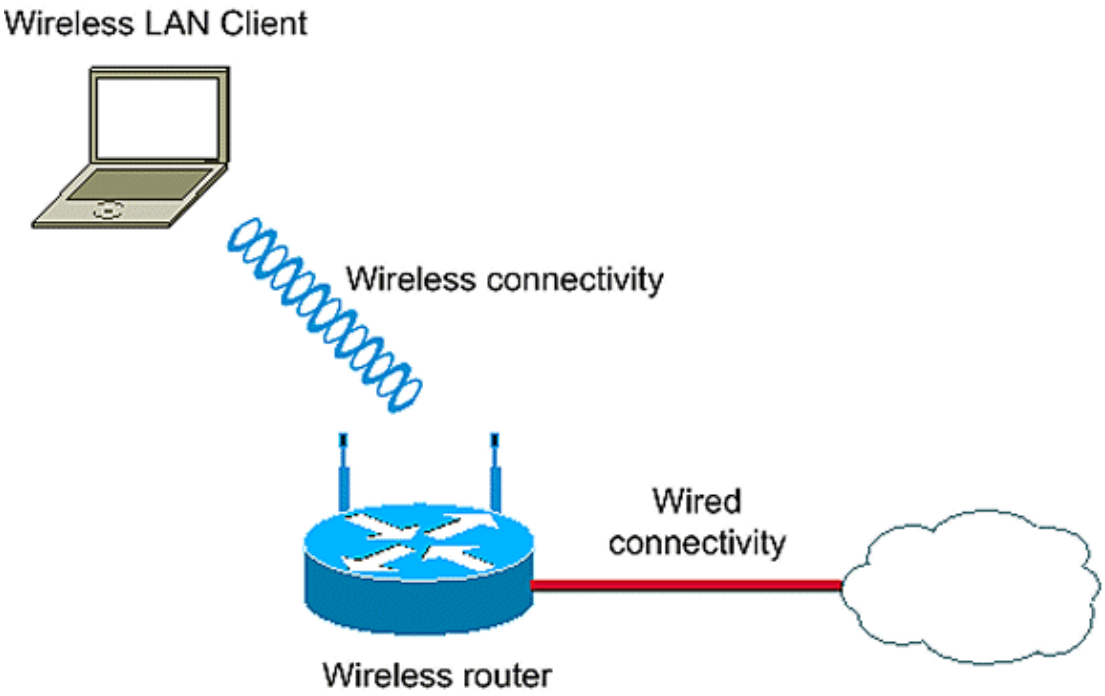
Note: This document does not focus on shared authentication since it is a less secured authentication type.

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) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



This setup uses the local RADIUS server on the Wireless ISR to authenticate Wireless clients with 802.1x authentication.

Configure Open Authentication

Open authentication is a null authentication algorithm. The access point grants any request for authentication. Open authentication allows any device network access. If no encryption is enabled on the network, any device that knows the SSID of the access point can gain access to the network. With WEP encryption enabled on an access point, the WEP key itself becomes a means of access control. If a device does not have the correct WEP key, even though authentication is successful, the device is unable to transmit data through the access point. Neither can it decrypt data sent from the access point.

This example configuration just explains a simple open authentication. The WEP key can be made mandatory or optional. This example configures WEP key as optional so that any device that does not use WEP can also authenticate and associate with this AP.

Refer to Open Authentication for more information.

This example uses this configuration setup to configure open authentication on the ISR.

- SSID name: "**open**"
- VLAN 1
- Internal DHCP server range: **10.1.0.0/16**

Note: For the sake of simplicity, this example does not use any encryption technique for authenticated clients.

Complete these actions on the router:

1. Configure the Integrated Routing and Bridging (IRB) and Set up the Bridge Group
2. Configure the Bridged Virtual Interface (BVI)
3. Configure the SSID for Open Authentication
4. Configure the Internal DHCP Server for the Wireless Clients of this VLAN

Configure the Integrated Routing and Bridging (IRB) and Set up the Bridge Group

Complete these actions:

1. **Enable IRB in the router.**

   router<configure>#**bridge irb**

   Note: If all the security types are to be configured on a single router, it is enough to enable IRB only once globally on the router. It does not need to be enabled for each individual authentication type.
2. **Define a bridge group.**

   This example uses the bridge−group number **1**.

   router<configure>#**bridge** *1*
3. **Choose the spanning tree protocol for the bridge group.**

   Here, IEEE spanning tree protocol is configured for this bridge group.

   router<configure>#**bridge** *1* **protocol** *ieee*
4. **Enable a BVI to accept and route routable packets received from its correspondent bridge group.**

   This example enables the BVI to accept and route the IP packet.

   router<configure>#**bridge** *1* **route** *ip*

Configure the Bridged Virtual Interface (BVI)

Complete these actions:

1. **Configure the BVI.**

   Configure the BVI when you assign the correspondent number of the bridge group to the BVI. Each bridge group can only have one corresponding BVI. This example assigns bridge group number 1 to the BVI.

   router<configure>#**interface BVI** *<1>*
2. **Assign an IP address to the BVI.**

   router<config−if>#**ip address** *10.1.1.1 255.255.0.0*

   router<config−if>#**no shut**

Refer to Configure Bridging for detailed information on bridging.

Configure the SSID for Open Authentication

Complete these actions:

1. **Enable the radio interface**

   In order to enable the radio interface, go to the DOT11 radio interface configuration mode and assign an SSID to the interface.

   router<config>#**interface dot11radio0**

   router<config−if>#**no shutdown**

   router<config−if>#**ssid** *open*

   The open authentication type can be configured in combination with MAC address authentication. In this case, the access point forces all client devices to perform MAC−address authentication before they are allowed to join the network.

   Open authentication can also be configured along with EAP authentication. The access point forces all client devices to perform EAP authentication before they are allowed to join the network. For the list−name, specify the authentication method list.

   An access point configured for EAP authentication forces all client devices that associate to perform EAP authentication. Client devices that do not use EAP cannot use the access point.
2. **Bind SSID to a VLAN.**

   In order to enable the SSID on this interface, bind the SSID to the VLAN in SSID configuration mode.

   router<config−ssid>**vlan** *1*
3. **Configure the SSID with open authentication.**

   router<config−ssid>#**authentication open**
4. **Configure the radio interface for the WEP key optional.**

   router<config>#**encryption vlan** *1* **mode WEP optional**
5. **Enable VLAN on the radio interface.**

   router<config>#**interface Dot11Radio 0.1**

   router<config−subif>#**encapsulation dot1Q** *1*

   router<config−subif>#**bridge−group** *1*

Configure the Internal DHCP Server for the Wireless Clients of this VLAN

Type these commands in the global configuration mode to configure the internal DHCP server for the wireless clients of this VLAN:

- **ip dhcp excluded−address 10.1.1.1 10.1.1.5**
- **ip dhcp pool** *open*

In the DHCP pool configuration mode, type these commands:

- **network** *10.1.0.0 255.255.0.0*
- **default−router** *10.1.1.1*

Configure 802.1x/EAP Authentication

This authentication type provides the highest level of security for your wireless network. With the Extensible Authentication Protocol (EAP) used to interact with an EAP−compatible RADIUS server, the access point helps a wireless client device and the RADIUS server to perform mutual authentication and derive a dynamic unicast WEP key. The RADIUS server sends the WEP key to the access point, which uses it for all unicast data signals that it sends to or receives from the client.

Refer to EAP Authentication for more information.

This example uses this configuration setup:

- SSID name: **leap**
- VLAN 2
- Internal DHCP server range: **10.2.0.0/16**

This example uses LEAP authentication as the mechanism to authenticate the wireless client.

Note: Refer to Cisco Secure ACS for Windows v3.2 With EAP−TLS Machine Authentication to configure EAP−TLS.

Note: Refer to Configuring Cisco Secure ACS for Windows v3.2 With PEAP−MS−CHAPv2 Machine Authentication to configure PEAP−MS−CHAPv2.

Note: Understand that all the configuration of these EAP types mainly involves the configuration changes at the client side and at the authentication server side. The configuration at the wireless router or the access point more or less remains the same for all these authentication types.

Note: As mentioned initially, this setup uses the local RADIUS server on the Wireless ISR to authenticate Wireless clients with 802.1x authentication.

Complete these actions on the router:

1. Configure the Integrated Routing and Bridging (IRB) and Set up the Bridge Group
2. Configure the Bridged Virtual Interface (BVI)
3. Configure the Local RADIUS Server for EAP Authentication
4. Configure the SSID for 802.1x/EAP Authentication
5. Configure the Internal DHCP Server for the Wireless Clients of this VLAN

Configure the Integrated Routing and Bridging (IRB) and Set up the Bridge Group

Complete these actions:

1. **Enable IRB in the router.**

   router<configure>#**bridge irb**

Note: If all the security types are to be configured on a single router, it is enough to enable IRB only once globally on the router. It does not need to be enabled for each individual authentication type.

2. **Define a bridge group.**

   This example uses the bridge−group number 2.

   router<configure>#**bridge** *2*
3. **Choose the spanning tree protocol for the bridge group.**

   Here, the IEEE spanning tree protocol is configured for this bridge group.

   router<configure>#**bridge** *2* **protocol** *ieee*
4. **Choose the spanning tree protocol for the bridge group.**

   Here, the IEEE spanning tree protocol is configured for this bridge group.

   router<configure>#**bridge** *2* **protocol** *ieee*
5. **Enable a BVI to accept and route routable packets that are received from its corresponding bridge group.**

   This example enables the BVI to accept and route IP packets.

   router<configure>#**bridge** *2* **route** *ip*

Configure the Bridged Virtual Interface (BVI)

Complete these actions:

1. **Configure the BVI.**

   Configure the BVI when you assign the correspondent number of the bridge group to the BVI. Each bridge group can only have one correspondent BVI. This example assigns bridge group number 2 to the BVI.

   router<configure>#**interface BVI** *<2>*
2. **Assign an IP address to the BVI.**

   router<config−if>#**ip address** *10.2.1.1 255.255.0.0*

   router<config−if>#**no shut**

Configure the Local RADIUS Server for EAP Authentication

As mentioned before, this document uses local RADIUS server on the wireless aware router for EAP authentication.

1. **Enable the authentication, authorization, and accounting (AAA) access control model.**

   router<configure>#**aaa new−model**
2. **Create a server group rad−eap for the RADIUS server.**

   router<configure>#**aaa group server radius** *rad−eap* **server** *10.2.1.1* **auth−port** *1812* **acct−port** *1813*

3. **Create a method list eap_methods that lists out the authentication method used to authenticate the AAA login user. Assign the method list to this server group.**

   router<configure>#**aaa authentication login** *eap_methods* **group** *rad−eap*
4. **Enable the router as a local authentication server and enter into configuration mode for the authenticator.**

   router<configure>#**radius−server local**
5. **In the Radius Server configuration mode, add the router as a AAA client of the local authentication server.**

   router<config−radsrv>#**nas** *10.2.1.1* **key** *Cisco*
6. **Configure user *user1* on the local Radius server.**

   router<config−radsrv>#**user** *user1* **password** *user1* **group** *rad−eap*
7. **Specify the RADIUS server host.**

   router<config−radsrv>#**radius−server host** *10.2.1.1* **auth−port** *1812* **acct−port** *1813* **key** *cisco*

   Note: This key should be the same as the one specified in **nas** command under radius−server configuration mode.

Configure the SSID for 802.1x/EAP Authentication

The configuration of the radio interface and the associated SSID for 802.1x/EAP involves the configuration of various wireless parameters on the router, which includes the SSID, the encryption mode, and the authentication type. This example uses the SSID called *leap*.

1. **Enable the radio interface.**

   In order to enable radio interface, go to the DOT11 radio interface configuration mode and assign an SSID to the interface.

   router<config>#**interface dot11radio0**

   router<config−if>#**no shutdown**

   router<config−if>#**ssid** *leap*
2. **Bind SSID to a VLAN.**

   In order to enable the SSID on this interface, bind the SSID to the VLAN in SSID configuration mode.

   router<config−ssid>#**vlan** *2*
3. **Configure the SSID with 802.1x/LEAP authentication.**

   router<config−ssid>#**authentication network−eap** *eap_methods*
4. **Configure the radio interface for dynamic key management.**

   router<config>#**encryption vlan** *2* **mode ciphers wep40**
5. **Enable VLAN on the radio interface.**

   router<config>#**interface Dot11Radio 0.2**

router<config−subif>#**encapsulation dot1Q** *2*

router<config−subif>#**bridge−group** *2*

Configure the Internal DHCP Server for the Wireless Clients of this VLAN

Type these commands in the global configuration mode to configure the internal DHCP server for the wireless clients of this VLAN:

- **ip dhcp excluded−address 10.2.1.1 10.2.1.5**
- **ip dhcp pool** *leapauth*

In the DHCP pool configuration mode, type these commands:

- **network** *10.2.0.0 255.255.0.0*
- **default−router** *10.2.1.1*

WPA Key Management

Wi−Fi Protected Access is a standards−based, interoperable security enhancement that strongly increases the level of data protection and access control for current and future wireless LAN systems.

Refer to WPA Key Management for more information.

WPA key management supports two mutually exclusive management types: WPA−Pre−Sshared key (WPA−PSK) and WPA (with EAP).

Configuring WPA−PSK

WPA−PSK is used as a key management type on a wireless LAN where 802.1x−based authentication is not available. In such networks, you must configure a pre−shared key on the access point. You can enter the pre−shared key as ASCII or hexadecimal characters. If you enter the key as ASCII characters, you enter between 8 and 63 characters, and the access point expands the key with the process described in the Password−based Cryptography Standard (RFC2898). If you enter the key as hexadecimal characters, you must enter 64 hexadecimal characters.

This example uses this configuration setup:

- SSID name: **wpa−shared**
- VLAN 3
- Internal DHCP server range: **10.3.0.0/16**

Complete these actions on the router:

1. Configure the Integrated Routing and Bridging (IRB) and Set up the Bridge Group
2. Configure the Bridged Virtual Interface (BVI)
3. Configure the SSID for WPA−PSK Authentication
4. Configure the Internal DHCP Server for the Wireless Clients of this VLAN

Configure the Integrated Routing and Bridging (IRB) and Set up the Bridge Group

Complete these actions:

1. **Enable IRB in the router.**

   router<configure>#**bridge irb**

   Note: If all the security types are to be configured on a single router, it is enough to enable IRB only once globally on the router. It does not need to be enabled for each individual authentication type.
2. **Define a bridge group.**

   This example uses the bridge−group number **3**.

   router<configure>#**bridge** *3*
3. **Choose the spanning tree protocol for the bridge group.**

   The IEEE spanning tree protocol is configured for this bridge group.

   router<configure>#**bridge** *3* **protocol** *ieee*
4. **Enable a BVI to accept and route routable packets received from its correspondent bridge group.**

   This example enables the BVI to accept and route IP packets.

   router<configure>#**bridge** *3* **route** *ip*

Configure the Bridged Virtual Interface (BVI)

Complete these actions:

1. **Configure the BVI.**

   Configure the BVI when you assign the correspondent number of the bridge group to the BVI. Each bridge group can only have one correspondent BVI. This example assigns bridge group number 3 to the BVI..

   router<configure>#**interface BVI** *<2>*
2. **Assign an IP address to the BVI.**

   router<config−if>#**ip address** *10.3.1.1 255.255.0.0*

   router<config−if>#**no shut**

Configure the SSID for WPA−PSK Authentication

Complete these actions:

1. **Enable the radio interface.**

   In order to enable the radio interface, go to the DOT11 radio interface configuration mode and assign an SSID to the interface.

   router<config>#**interface dot11radio0**

router<config−if>#**no shutdown**

router<config−if>#**ssid** *wpa−shared*

2. **In order to enable WPA key management, first configure the WPA encryption cipher for the VLAN interface. This example uses tkip as the encryption cipher.**.

   Type this command to specify the WPA key management type on the radio interface.

   router<config>#**interface dot11radio0**

   router(config−if)#**encryption vlan** *3* **mode ciphers** *tkip*
3. **Bind SSID to a VLAN.**

   In order to enable the SSID on this interface, bind the SSID to the VLAN in SSID configuration mode.

   router<config−ssid>**vlan** *3*
4. **Configure the SSID with WPA−PSK authentication.**

   You need to configure open or network EAP authentication first in the SSID configuration mode to enable WPA key management. This example configures open authentication.

   router<config>#**interface dot11radio0**

   router<config−if>#**ssid** *wpa−shared*

   router<config−ssid>#**authentication open**

   Now, enable WPA key management on the SSID. The key management cipher tkip is already configured for this VLAN.

   router(config−if−ssid)#**authentication key−management wpa**

   Configure the WPA−PSK authentication on the SSID.

   router(config−if−ssid)#**wpa−psk ascii** *1234567890* ***!−−− 1234567890 is the pre−shared key value for this SSID. Ensure that the same key is specified for this SSID at the client side.***
5. **Enable VLAN on the radio interface.**

   router<config>#**interface Dot11Radio 0.3**

   router<config−subif>#**encapsulation dot1Q** *3*

   router<config−subif>#**bridge−group** *3*

Configure the Internal DHCP Server for the Wireless Clients of this VLAN

Type these commands in the global configuration mode to configure the internal DHCP server for the wireless clients of this VLAN:

- **ip dhcp excluded−address 10.3.1.1 10.3.1.5**
- **ip dhcp pool** *wpa−psk*

In the DHCP pool configuration mode, type these commands:

- **network** *10.3.0.0 255.255.0.0*
- **default−router** *10.3.1.1*

Configure WPA (with EAP) Authentication

This is another WPA key management type. Here, clients and the authentication server authenticate to each other with an EAP authentication method, and the client and server generate a pairwise master key (PMK). With WPA, the server generates the PMK dynamically and passes it to the access point, but, with WPA−PSK, you configure a pre−shared key on both the client and the access point, and that pre−shared key is used as the PMK.

Refer to WPA with EAP Authentication for more information.

This example uses this configuration setup:

- SSID name: **wpa−dot1x**
- VLAN 4
- Internal DHCP server range: **10.4.0.0/16**

Complete these actions on the router:

1. Configure the Integrated Routing and Bridging (IRB) and Set up the Bridge Group
2. Configure the Bridged Virtual Interface (BVI)
3. Configure the Local RADIUS Server for WPA Authentication.
4. Configure the SSID for WPA with EAP Authentication
5. Configure the Internal DHCP Server for the Wireless Clients of this VLAN

Configure the Integrated Routing and Bridging (IRB) and Set up the Bridge Group

Complete these actions:

1. **Enable IRB in the router.**

   router<configure>#**bridge irb**

   Note: If all the security types are to be configured on a single router, it is enough to enable IRB only once globally on the router. It does not need to be enabled for each individual authentication type.
2. **Define a Bridge group.**

   This example uses bridge−group number **4**.

   router<configure>#**bridge** *4*
3. **Select the spanning tree protocol for the bridge group.**

   Here, the IEEE spanning tree protocol is configured for this bridge group.

   router<configure>#**bridge** *4* **protocol** *ieee*
4. **Enable a BVI to accept and route the routable packets received from its correspondent bridge group.**

   This example enables the BVI to accept and route IP packets.

router<configure>#**bridge** *4* **route** *ip*

Configure the Bridged Virtual Interface (BVI)

Complete these actions:

1. **Configure the BVI.**

   Configure the BVI when you assign the correspondent number of the bridge group to the BVI. Each bridge group can only have one corresponding BVI. This example assigns bridge group number 4 to the BVI.

   router<configure>#**interface BVI** *<4>*
2. **Assign an IP address to the BVI.**

   router<config−if>#**ip address** *10.4.1.1 255.255.0.0*

   router<config−if>#**no shut**

Configure the Local RADIUS Server for WPA Authentication

Refer to the section under 802.1x/EAP Authentication for the detailed procedure.

Configure the SSID for WPA with EAP Authentication

Complete these actions:

1. **Enable the Radio interface.**

   In order to enable radio interface, go to the DOT11 radio interface configuration mode and assign an SSID to the interface.

   router<config>#**interface dot11radio0**

   router<config−if>#**no shutdown**

   router<config−if>#**ssid** *wpa−dot1x*
2. **In order to enable WPA key management, first configure the WPA encryption cipher for the VLAN interface. This example uses tkip as the encryption cipher.**.

   Type this command to specify the WPA key management type on the radio interface.

   router<config>#**interface dot11radio0**

   router(config−if)#**encryption vlan** *4* **mode ciphers** *tkip*
3. **Bind SSID to a VLAN.**

   In order to enable the SSID on this interface, bind the SSID to the VLAN in the SSID configuration mode.

   vlan *4*
4. **Configure the SSID with the WPA−PSK authentication.**

In order to configure the radio interface for WPA with EAP authentication, first configure the associated SSID for network EAP.

router<config>#**interface dot11radio0**

router<config−if>#**ssid** *wpa−shared*

router<config−ssid>#**authentication network eap** *eap_methods*

5. **Now, enable the WPA key management on the SSID. The key management cipher tkip is already configured for this VLAN.**

   router(config−if−ssid)#**authentication key−management wpa**
6. **Enable VLAN on the radio interface.**

   router<config>#**interface Dot11Radio 0.4**

   router<config−subif>#**encapsulation dot1Q** *4*

   router<config−subif>#**bridge−group** *4*

Configure the Internal DHCP Server for the Wireless Clients of this VLAN

Type these commands in the global configuration mode to configure the internal DHCP server for the wireless clients of this VLAN:

- **ip dhcp excluded−address 10.4.1.1 10.4.1.5**
- **ip dhcp pool** *wpa−dot1shared*

In the DHCP pool configuration mode, type these commands:

- **network** *10.4.0.0 255.255.0.0*
- **default−router** *10.4.1.1*

Configure Wireless Client for Authentication

After you configure the ISR, configure the wireless client for different authentication types as explained so that the router can authenticate these wireless clients and provide access to the WLAN network. This document uses Cisco Aironet Desktop Utility (ADU) for client−side configuration.

Configure the Wireless Client for Open Authentication

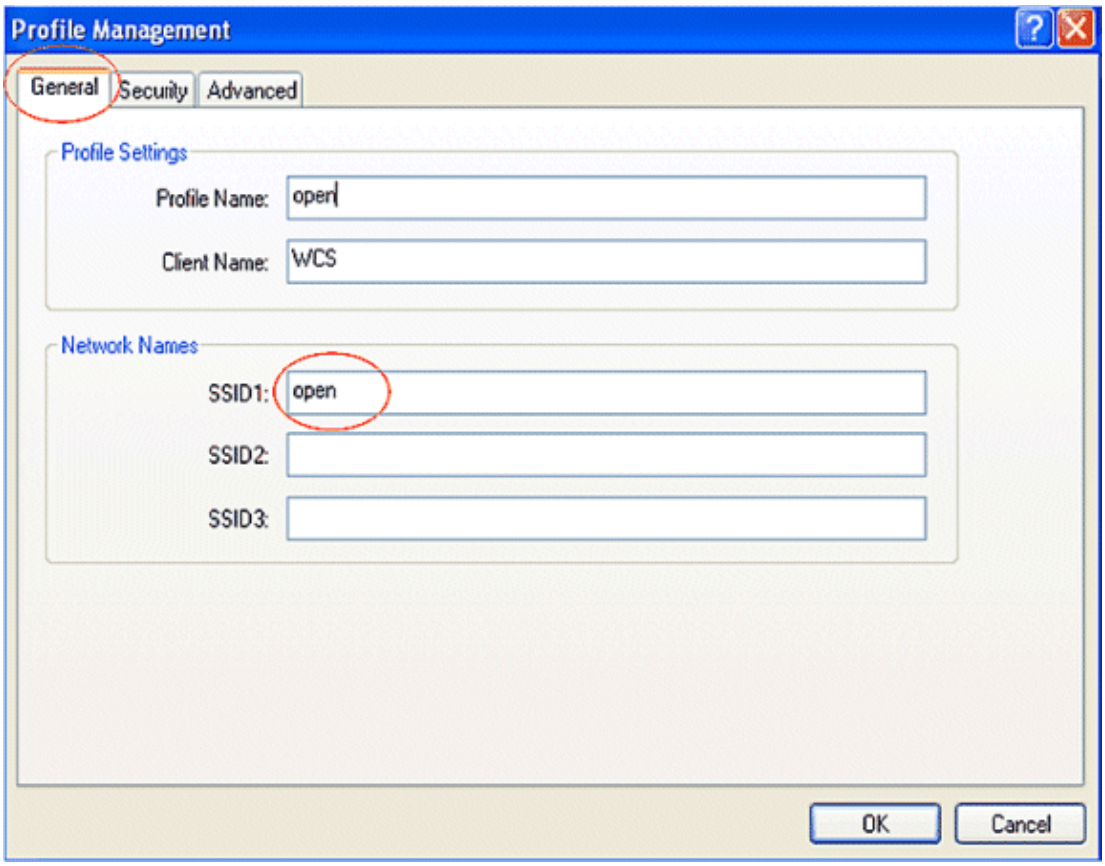
Complete these steps:

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 open authentication. Under the **General** tab, enter the Profile Name and the SSID that the client adapter uses.

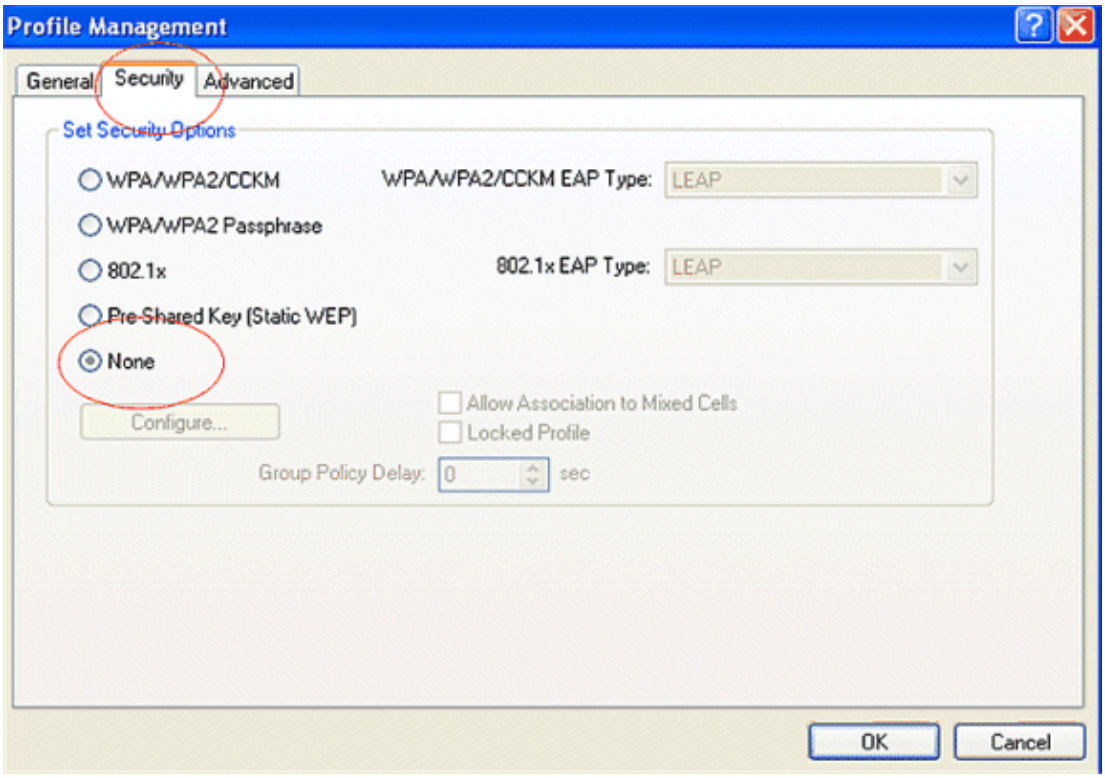
   In this example, the profile name and SSID are **open**.

   Note: The SSID must match the SSID that you configured on the ISR for open authentication.

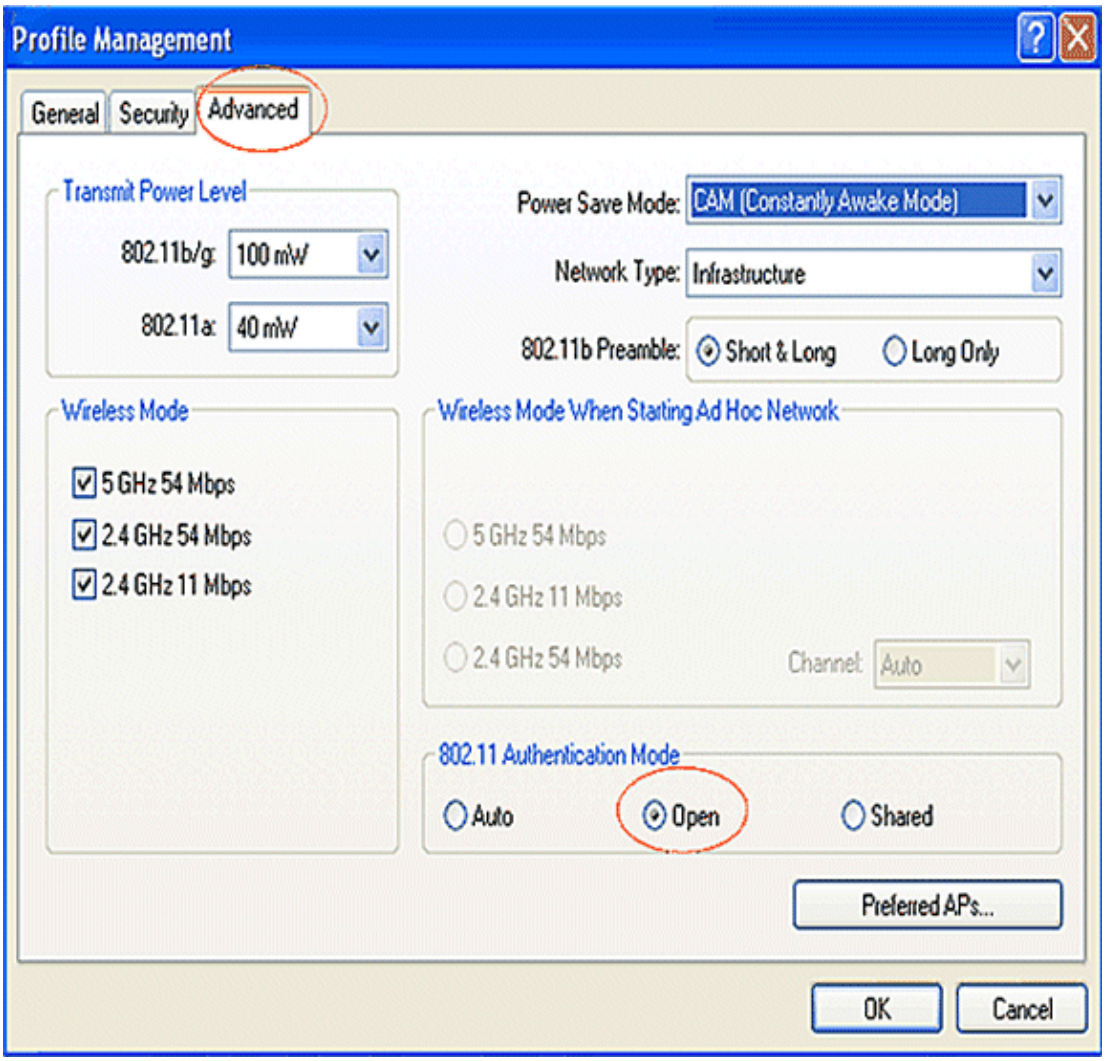


2. Click the **Security** tab and leave the security option as **None** for WEP encryption. Since this example uses WEP as optional, setting this option to None will allow the client to successfully associate and communicate with the WLAN network.

   Click **OK**

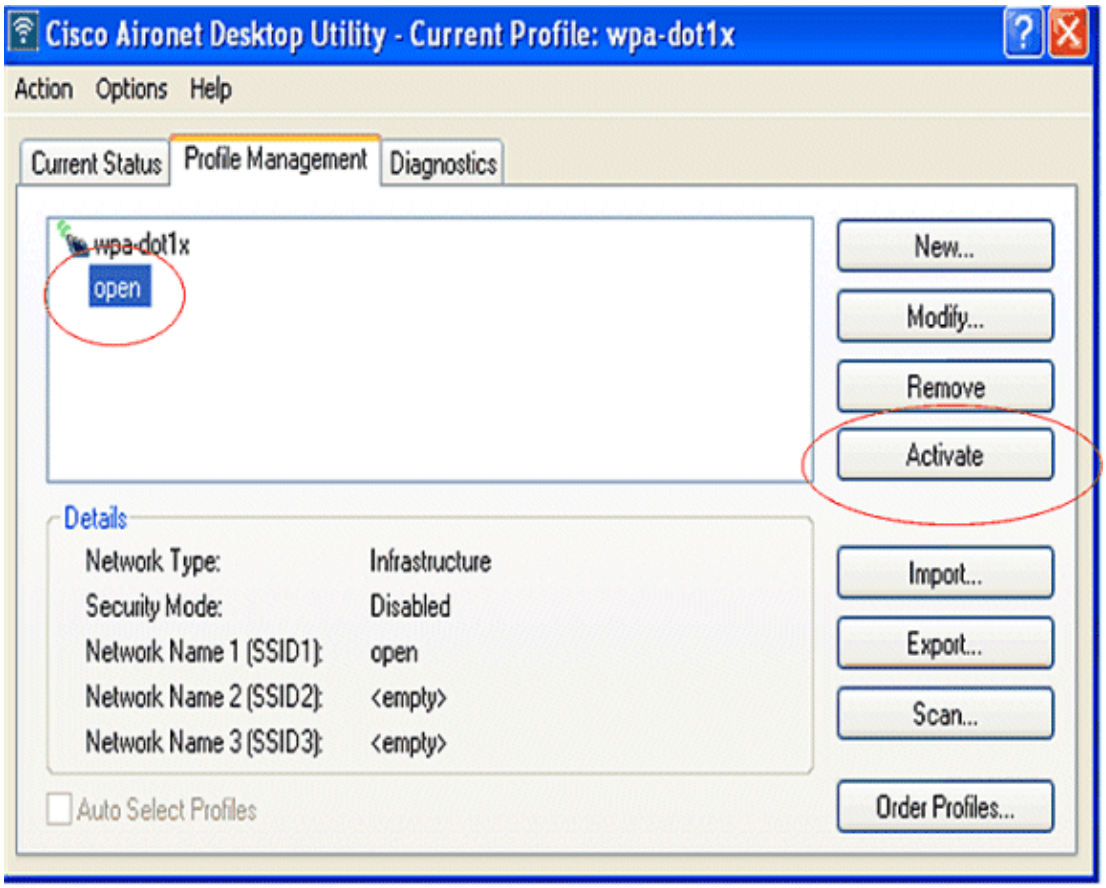


3. Select **Advanced window** from the **Profile Management** tab and set 802.11 Authentication Mode as **Open** for open authentication.

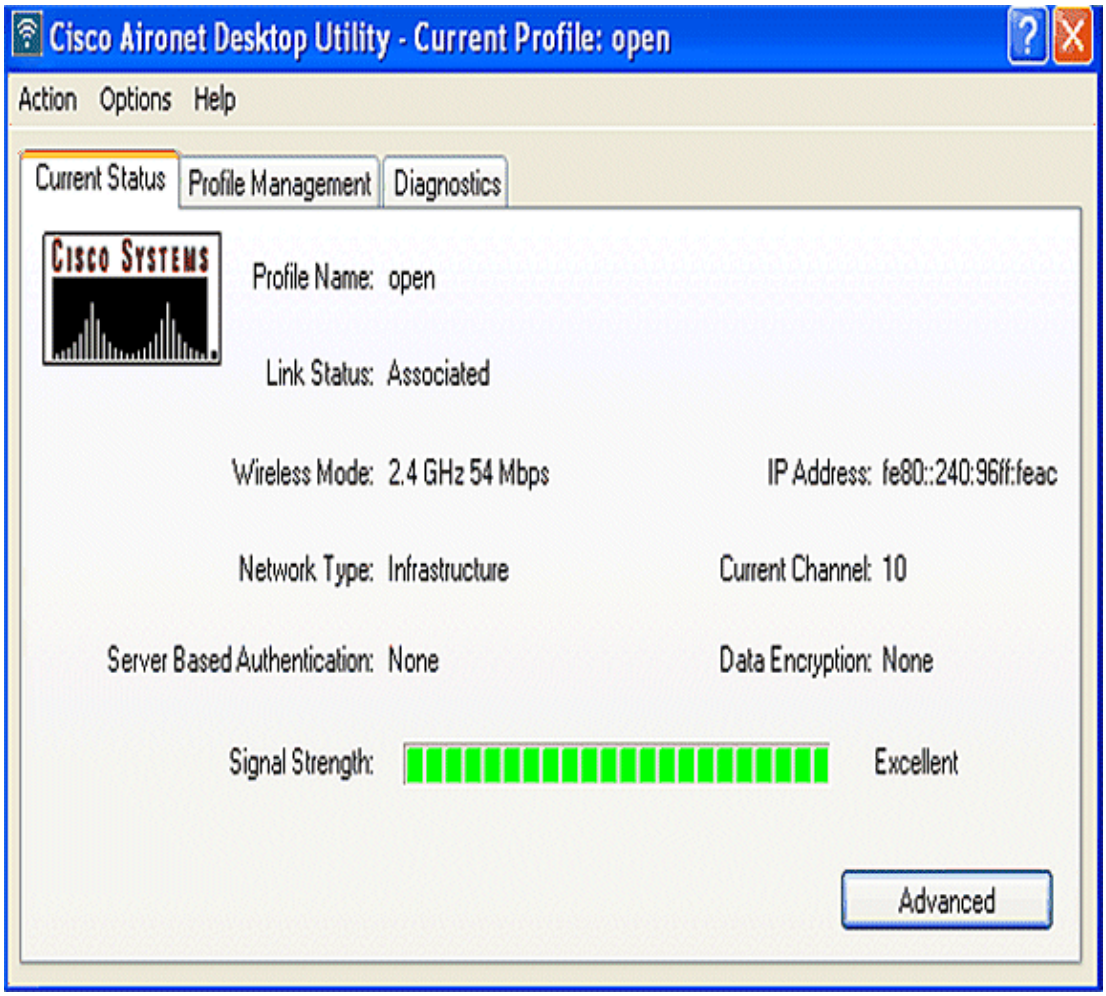


Use this section to confirm that your configuration works properly.

1. After the client profile is created, click **Activate** under the Profile Management tab to activate the profile.



2. Check the ADU status for a successful authentication.



Configure the Wireless Client for 802.1x/EAP Authentication

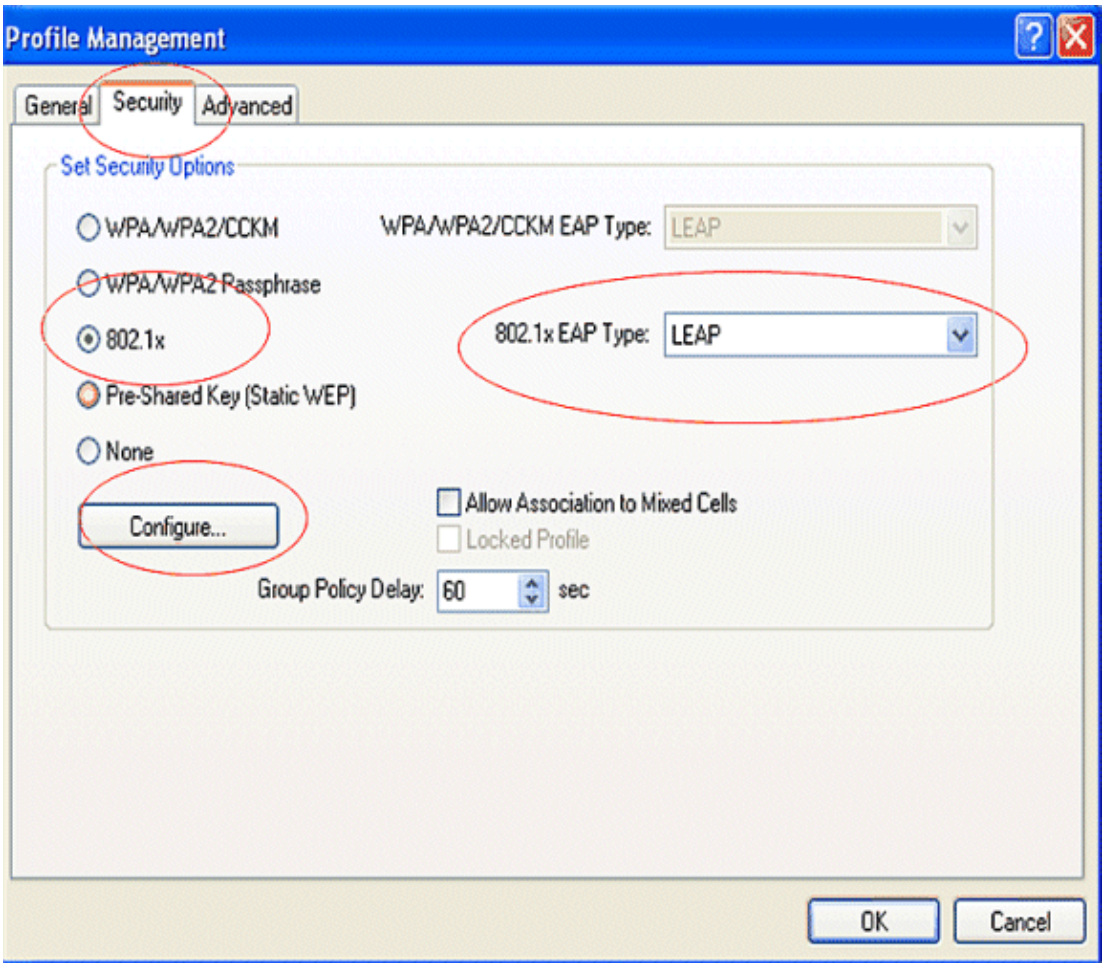
Complete these steps:

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

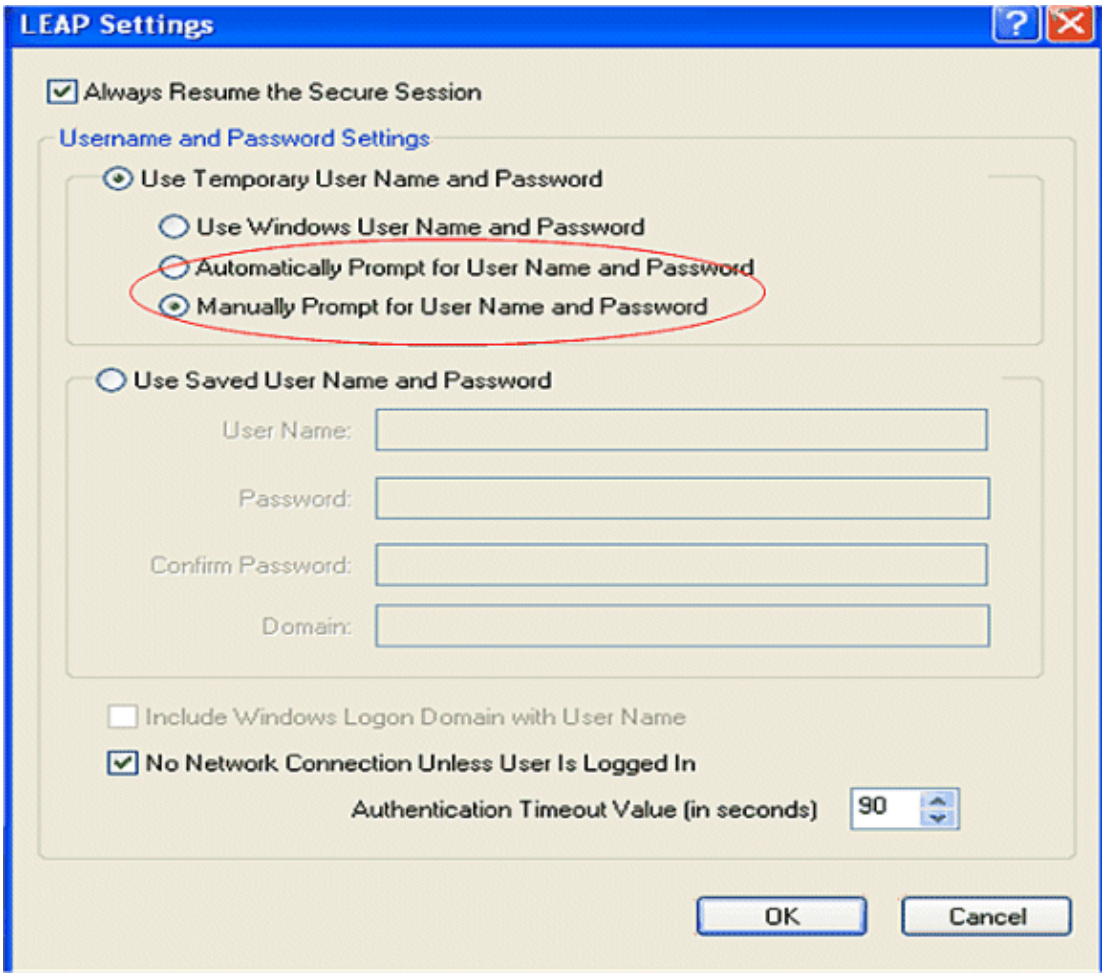
   A new window displays where you can set the configuration for open authentication. Under the **General** tab, enter the Profile Name and the SSID that the client adapter uses.

   In this example, the profile name and SSID are **leap**.
2. Under **Profile Management**, click the **Security** tab, set the security option as 802.1x, and choose the appropriate EAP type. This document uses LEAP as the EAP type for authentication. Now, click **Configure** to configure LEAP username and password settings.

   Note: Note: The SSID must match the SSID that you configured on the ISR for 802.1x/EAP authentication.

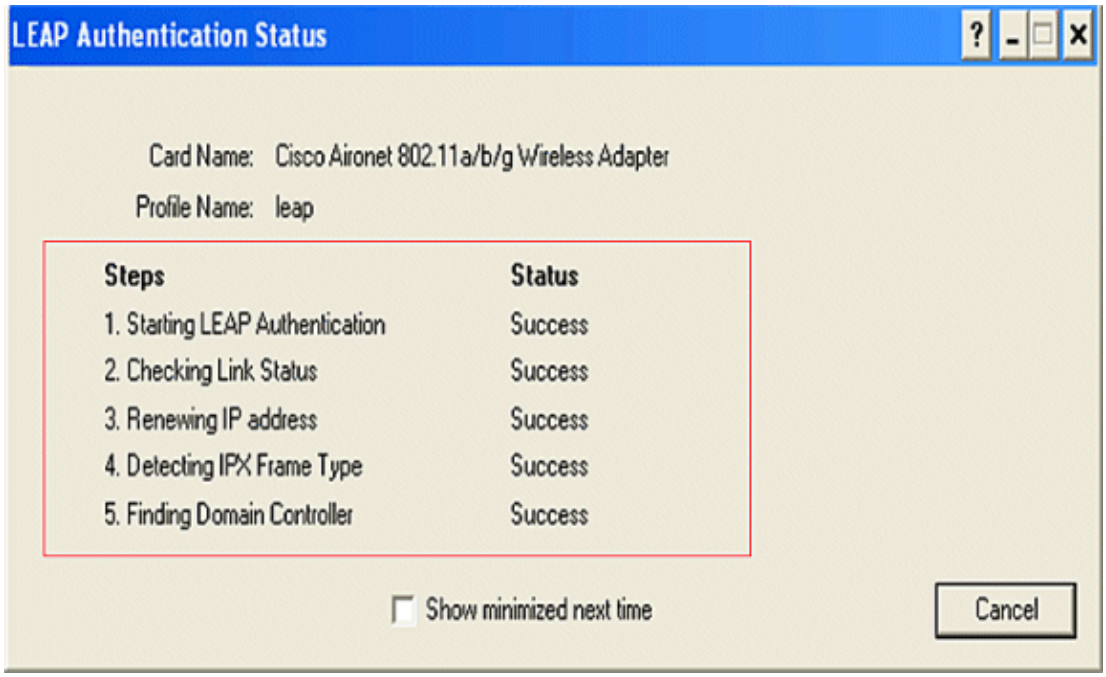


3. Under username and password settings, this example chooses to **Manually Prompt for User Name and Password** so that the client is prompted to enter the correct user name and password while the client tries to connect to the network. Click **OK**.



Use this section to confirm that your configuration works properly.

- After the client profile is created, click **Activate** under the **Profile Management** tab to activate the profile **leap**. You are prompted for the **leap** user name and password. This example uses the username and password **user1**. Click **OK**.
- You can watch the client authenticate successfully and be assigned an IP address from the DHCP server configured on the router.



Configure the Wireless Client for WPA−PSK Authentication

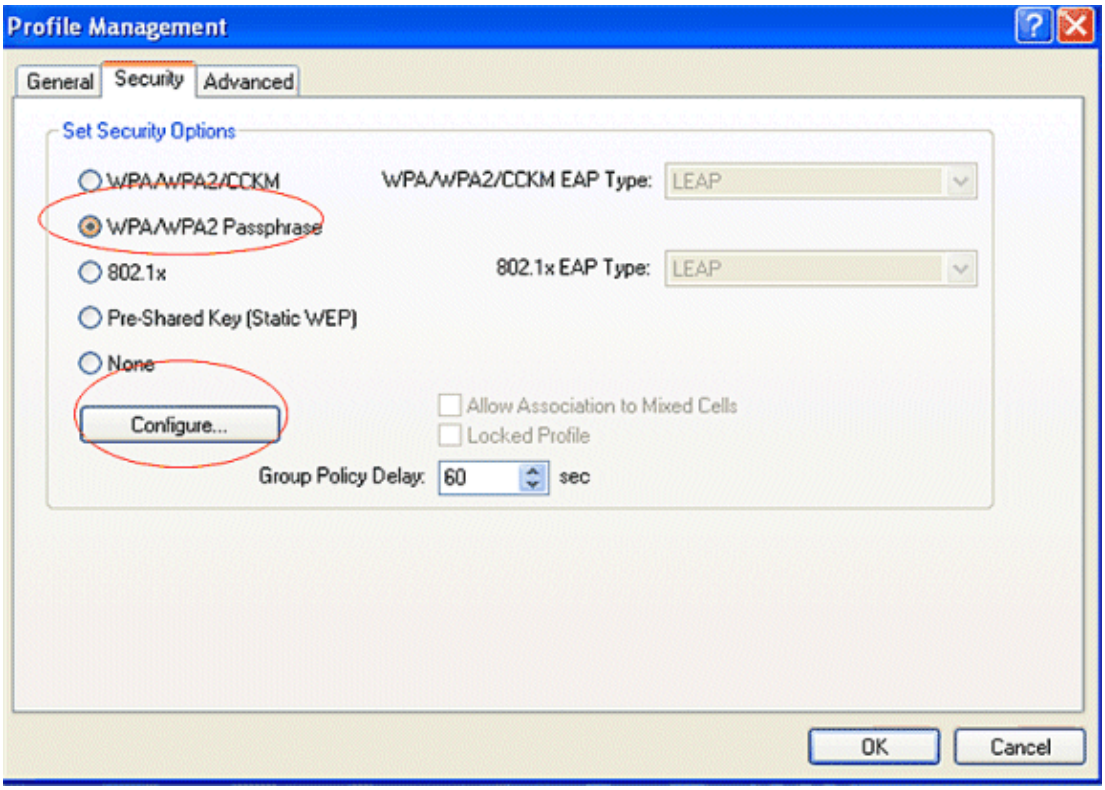
Complete these steps:

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

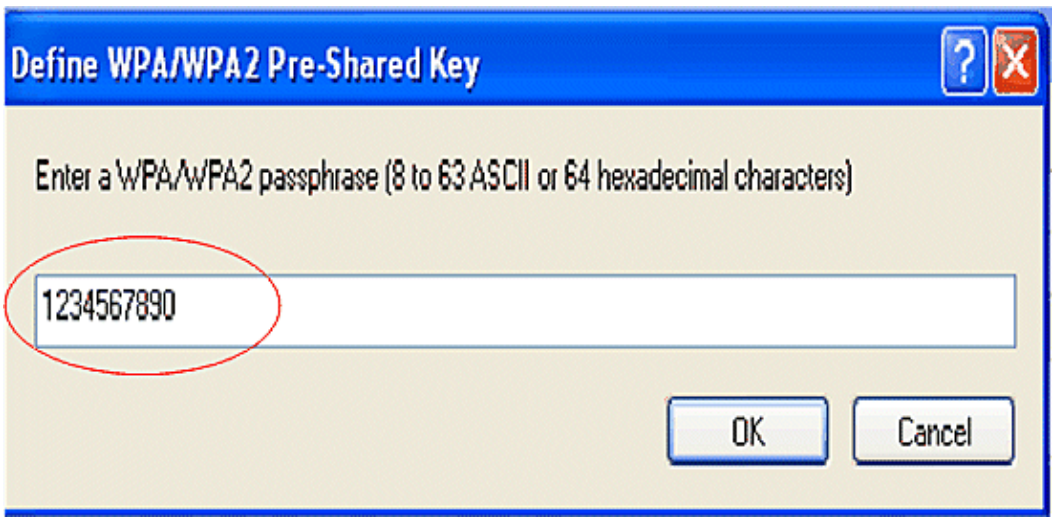
   A new window displays where you can set the configuration for open authentication. Under the **General** tab, enter the **Profile Name** and **SSID** that the client adapter uses.

   In this example, the profile name and SSID are **wpa−shared**.

   Note: The SSID must match the SSID that you configured on the ISR for WPA−PSK authentication.
2. Under **Profile Management**, click the **Security** tab and set the security option as **WPA/WPA2 Passphrase**. Now, click **Configure** to configure the WPA Passphrase.

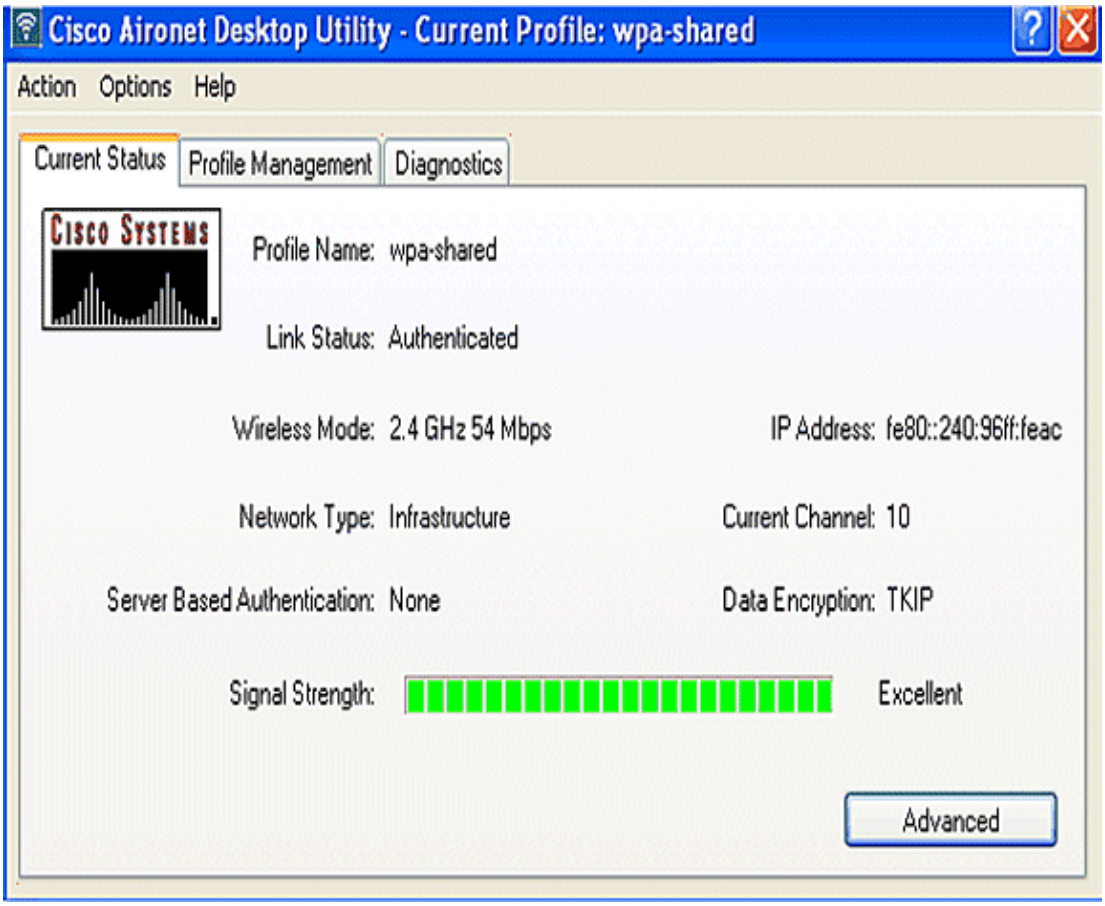


3. Define a WPA Pre−Shared Key. The key must be 8 to 63 ASCII characters in length. Click **OK** .



Use this section to confirm that your configuration works properly.

- After the client profile is created, click **Activate** under the **Profile Management** tab to activate the profile **wpa−shared**.
- Check the ADU for a successful authentication.



Configure the Wireless Client for WPA (with EAP) Authentication

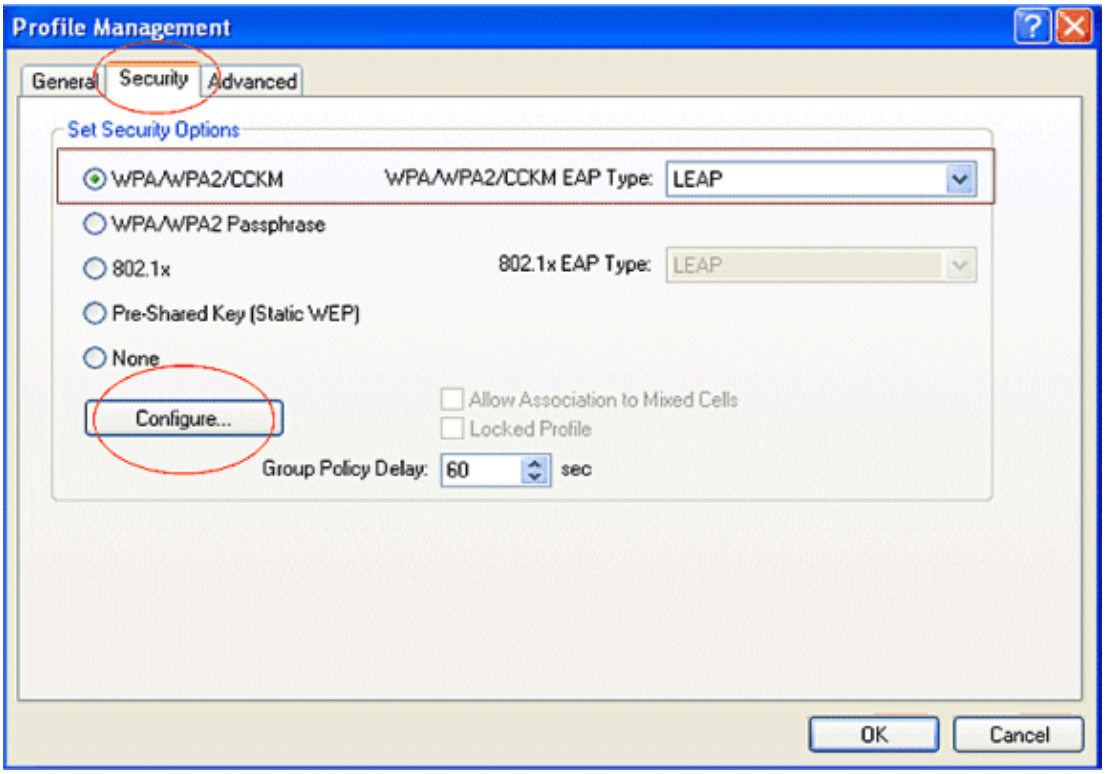
Complete these steps:

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

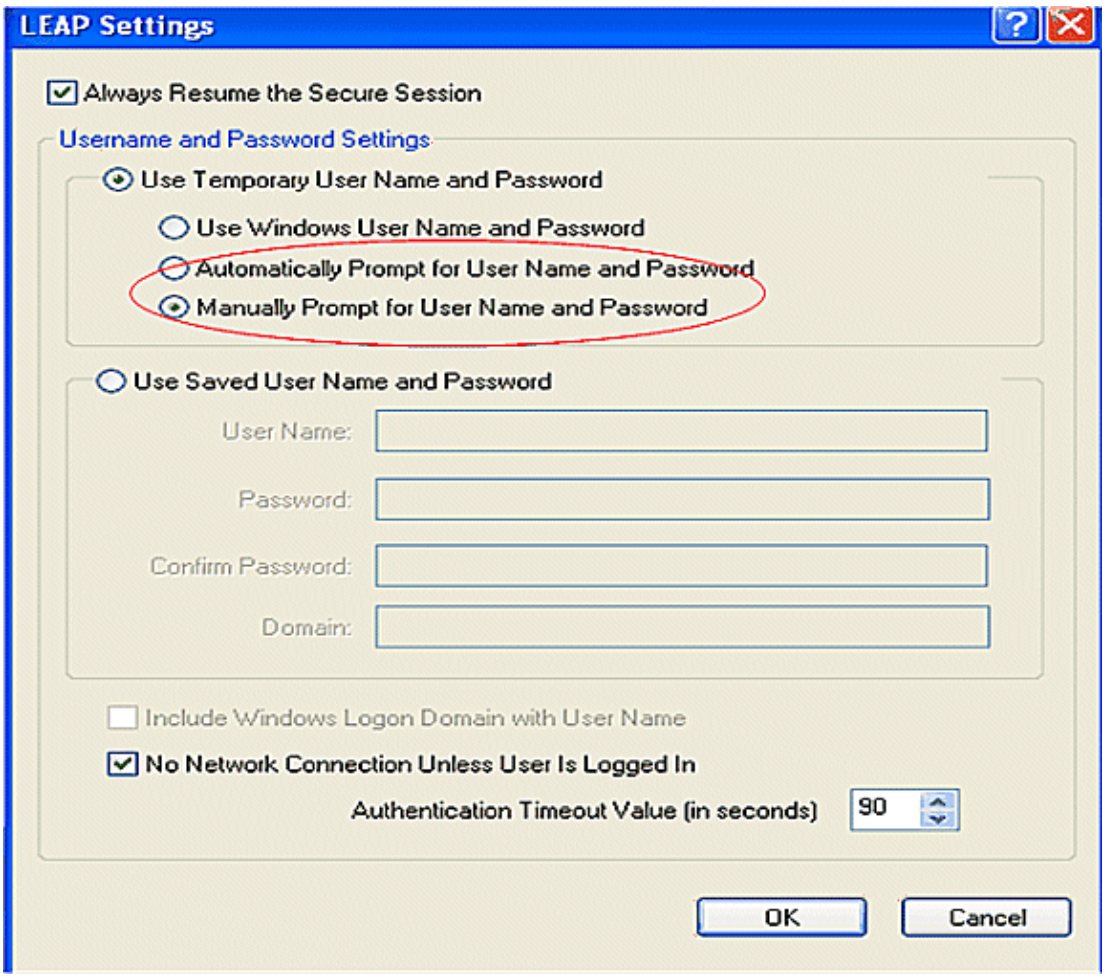
   A new window displays where you can set the configuration for open authentication. Under the **General** tab, enter the Profile Name and SSID that the client adapter uses.

   In this example, the profile name and SSID are **wpa−dot1x**.

   Note: The SSID must match the SSID that you configured on the ISR for WPA (with EAP) authentication.
2. Under **Profile Management**, click the **Security** tab, set the security option as **WPA/WPA2/CCKM**, and and choose the appropriate WPA/WPA2/CCKM EAP type. This document uses LEAP as the EAP type for authentication. Now, click **Configure** to configure LEAP username and password settings.

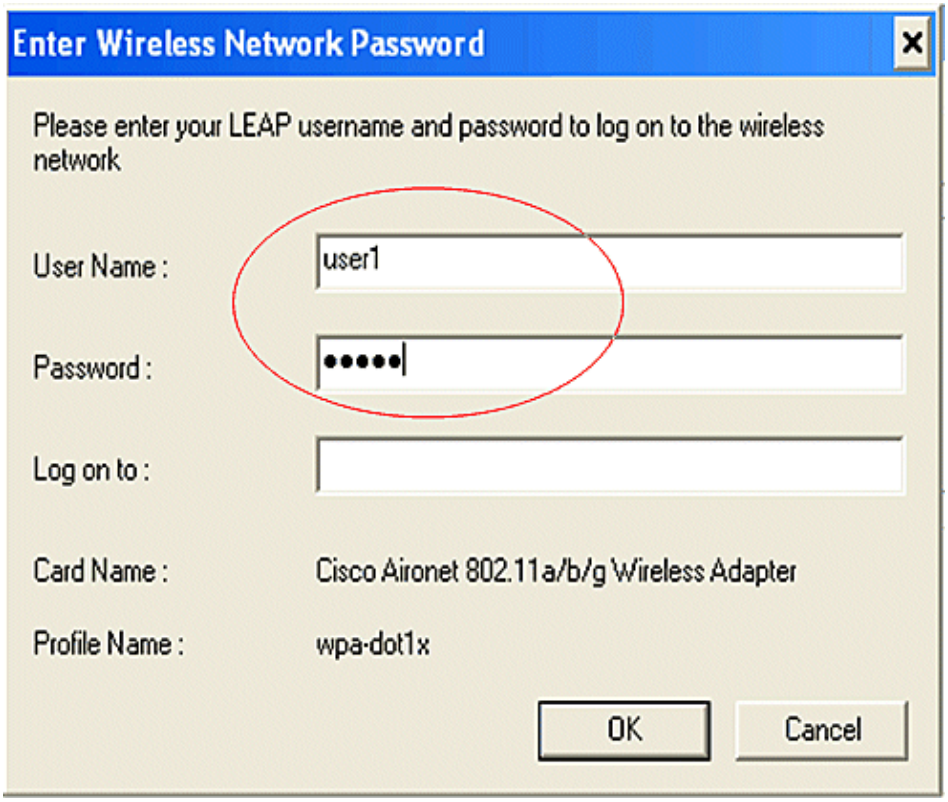


3. Under the Username and Password Settings area, this example chooses to **Manually Prompt for User Name and Password** so that the client is prompted to enter the correct user name and password while the client tries to connect to the network. Click **OK**.

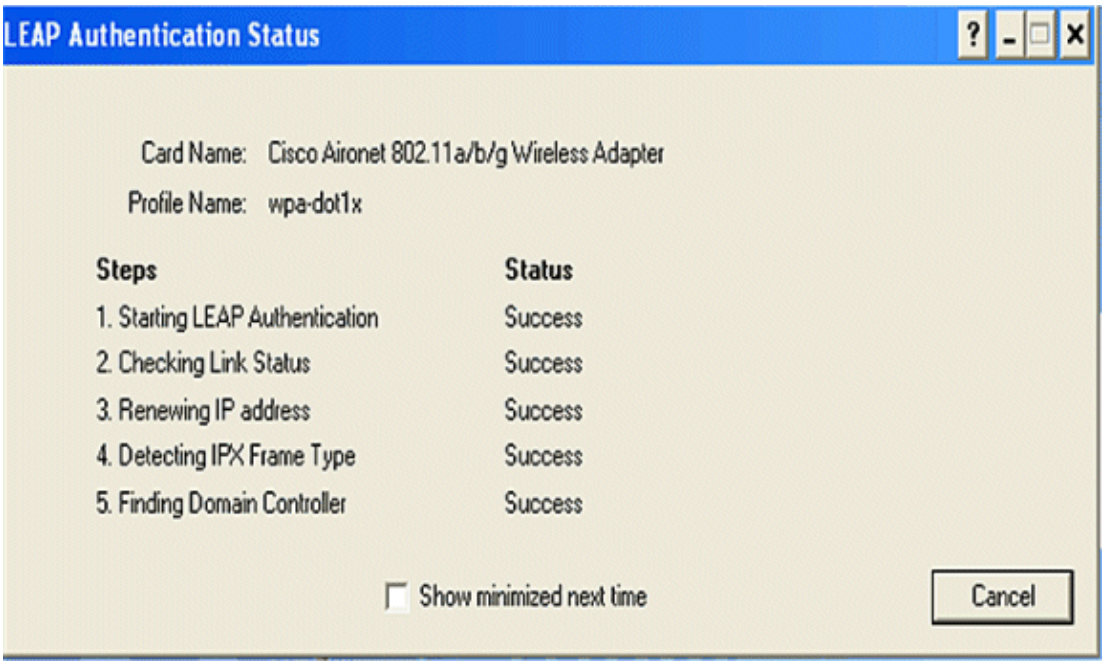


Use this section to confirm that your configuration works properly.

1. After the client profile is created, click **Activate** under the Profile Management tab to activate the profile **wpa−dot1x**. You are prompted for the LEAP user name and password. This example uses username and password as **user1**. Click **OK**.



2. You can watch the client authenticate successfully.



The command **show dot11 associations** from the router CLI displays full details on the client association status. Here is an example.

Router#**show dot11 associations**

```
802.11 Client Stations on Dot11Radio0:

SSID [leap] :

MAC Address    IP address      Device        Name            Parent         State
0040.96ac.e657 10.3.0.2        CB21AG/PI21AG WCS             self         EAP-Assoc

SSID [open] :

SSID [pre-shared] : DISABLED, not associated with a configured VLAN

SSID [wpa-dot1x] :

SSID [wpa-shared] :


Others:  (not related to any ssid)
```

Troubleshoot

Troubleshooting Commands

You can use these debug commands to troubleshoot your configuration.

- **debug dot11 aaa authenticator all** Activates the debugging of MAC and EAP authentication packets.
- **debug radius authentication** Displays the RADIUS negotiations between the server and client.
- **debug radius local-server packets** Displays the content of the RADIUS packets that are sent and received.
- **debug radius local-server client** Displays error messages about failed client authentications.

Related Information

- **Authentication on Wireless LAN Controllers Configuration Examples**
- **Configuring VLANs on Access Points**
- **1800 ISR Wireless Router with Internal DHCP and Open Authentication Configuration Example**
- **Cisco Wireless ISR and HWIC Access Point Configuration Guide**
- **Wireless LAN Connectivity using an ISR with WEP Encryption and LEAP Authentication Configuration Example**
- **Technical Support & Documentation − Cisco Systems**
- **Configuring Authentication Types**
- **Wireless LAN Connectivity Using an ISR with WEP Encryption and LEAP Authentication Configuration Example**

Updated: Apr 07, 2008 Document ID: 98499