Wi−Fi Protected Access (WPA) in a Cisco Unified Wireless Network Configuration Example

Document ID: 100708

Introduction

This document describes how to configure Wi−Fi Protected Access (WPA) in a Cisco Unified Wireless Network.

Prerequisites

Requirements

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

- WPA
- Wireless LAN (WLAN) security solutions

Note: Refer to Cisco 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 1000 Series Lightweight Access Point (LAP)
- Cisco 4404 Wireless LAN Controller (WLC) that runs firmware 4.2.61.0
- Cisco 802.11a/b/g client adapter that runs firmware 4.1
- Aironet Desktop Utility (ADU) that runs firmware 4.1
- Cisco Secure ACS server version 4.1

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.

WPA and WPA2 Support

The Cisco Unified Wireless Network includes support for the Wi−Fi Alliance certifications WPA and WPA2. WPA was introduced by the Wi−Fi Alliance in 2003. WPA2 was introduced by the Wi−Fi Alliance in 2004. All products Wi−Fi Certified for WPA2 are required to be interoperable with products that are Wi−Fi Certified for WPA.

WPA and WPA2 offer a high level of assurance for end users and network administrators that their data will remain private and that access to their networks will be restricted to authorized users. Both have personal and enterprise modes of operation that meet the distinct needs of the two market segments. The Enterprise Mode of each uses IEEE 802.1X and EAP for authentication. The Personal Mode of each uses Pre−Shared Key (PSK) for authentication. Cisco does not recommend Personal Mode for business or government deployments because it uses a PSK for user authentication. PSK is not secure for enterprise environments.

WPA addresses all known WEP vulnerabilities in the original IEEE 802.11 security implementation bringing an immediate security solution to WLANs in both enterprise and small office/home office (SOHO) environments. WPA uses TKIP for encryption.

WPA2 is the next generation of Wi−Fi security. It is the Wi−Fi Alliance's interoperable implementation of the ratified IEEE 802.11i standard. It implements the National Institute of Standards and Technology (NIST) recommended AES encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). WPA2 facilitates government FIPS 140−2 compliance.

	WPA	WPA2
Enterprise Mode (Business, Government, Education)	• Authentication: IEEE 802.1X/EAP • Encryption: TKIP/MIC	• Authentication: IEEE 802.1X/EAP • Encryption: AES−CCMP
Personal Mode (SOHO, Home/Personal)	• Authentication: PSK • Encryption: TKIP/MIC	• Authentication: PSK • Encryption: AES−CCMP

In Enterprise mode of operation both WPA and WPA2 use 802.1X/EAP for authentication. 802.1X provides

WLANs with strong, mutual authentication between a client and an authentication server. In addition, 802.1X provides dynamic per−user, per−session encryption keys, removing the administrative burden and security issues surrounding static encryption keys.

With 802.1X, the credentials used for authentication, such as logon passwords, are never transmitted in the clear, or without encryption, over the wireless medium. While 802.1X authentication types provide strong authentication for wireless LANs, TKIP or AES are needed for encryption in addition to 802.1X since standard 802.11 WEP encryption, is vulnerable to network attacks.

Several 802.1X authentication types exist, each providing a different approach to authentication while relying on the same framework and EAP for communication between a client and an access point. Cisco Aironet products support more 802.1X EAP authentication types than any other WLAN products. Supported types include:

- Cisco LEAP
- EAP−Flexible Authentication via Secure Tunneling (EAP−FAST)
- EAP−Transport Layer Security (EAP−TLS)
- Protected Extensible Authentication Protocol (PEAP)
- EAP−Tunneled TLS (EAP−TTLS)
- EAP−Subscriber Identity Module (EAP−SIM)

Another benefit of 802.1X authentication is centralized management for WLAN user groups, including policy−based key rotation, dynamic key assignment, dynamic VLAN assignment, and SSID restriction. These features rotate the encryption keys.

In the Personal mode of operation, a pre−shared key (password) is used for authentication. Personal mode requires only an access point and client device, while Enterprise mode typically requires a RADIUS or other authentication server on the network.

This document provides examples for configuring WPA2 (Enterprise mode) and WPA2−PSK (Personal mode) in a Cisco Unified Wireless network.

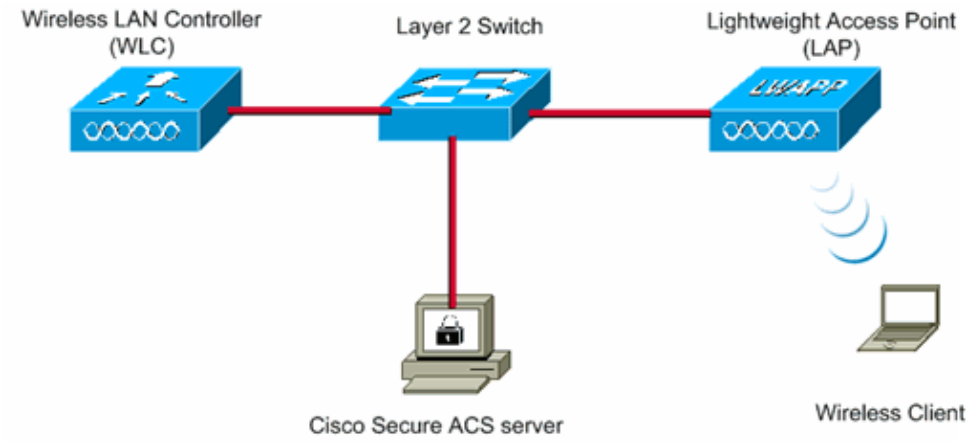
Network Setup

In this setup, a Cisco 4404 WLC and a Cisco 1000 Series LAP are connected through a Layer 2 Switch. An external RADIUS server (Cisco Secure ACS) is also connected to the same switch. All the devices are in the same subnet. The access point (LAP) is initially registered to the controller. Two Wireless LANs, one for WPA2 Enterprise mode and the other for WPA2 Personal mode, need to be created.

WPA2−Enterprise mode WLAN (SSID: WPA2−Enterprise) will use EAP−FAST for authenticating the Wireless clients and AES for encryption. Cisco Secure ACS server will be used as the external RADIUS server for authenticating the wireless clients.

WPA2−Personal mode WLAN (SSID: WPA2−PSK) will use WPA2−PSK for authentication with the pre−shared key abcdefghijk .

You need to configure the devices for this setup:



WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

Configure the Devices for WPA2 Enterprise Mode

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

Perform these steps in order to configure the devices for WPA2 Enterprise mode of operation:

1. Configure the WLC for RADIUS Authentication through an External RADIUS Server
2. Configure the WLAN for WPA2 Enterprise Mode Authentication (EAP−FAST)
3. Configure the Wireless Client for WPA2 Enterprise Mode

Configure the WLC for RADIUS Authentication through an External RADIUS Server

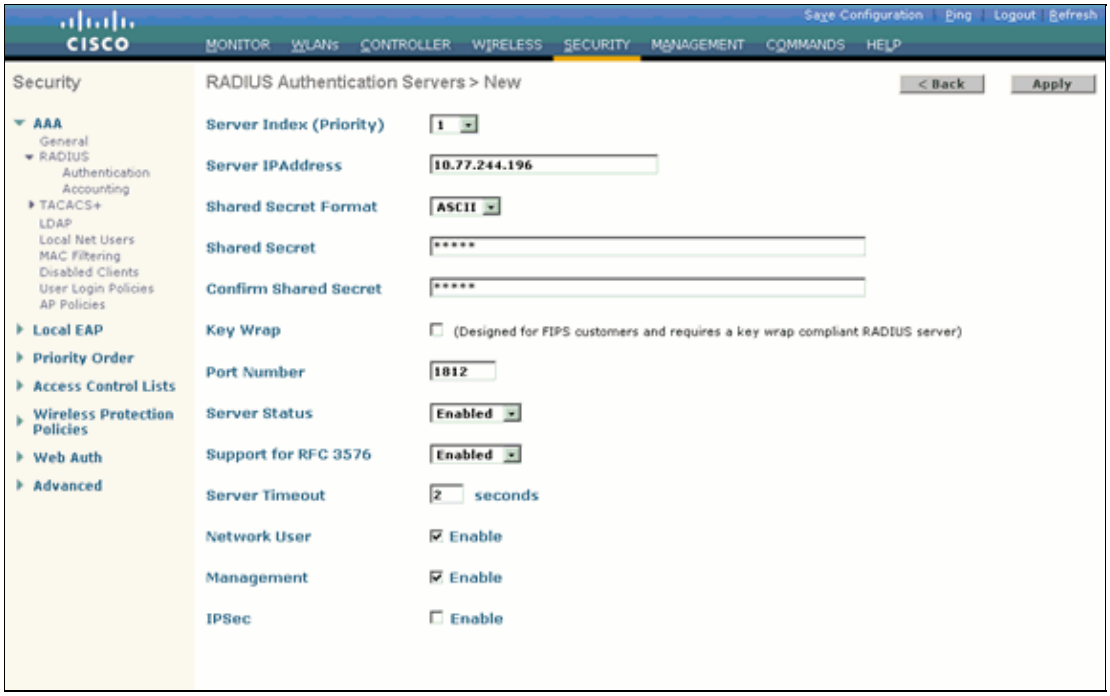
The WLC needs to be configured in order to forward the user credentials to an external RADIUS server. The external RADIUS server then validates the user credentials using EAP−FAST and provides access to the wireless clients.

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.
2. Define the RADIUS server parameters on the **RADIUS Authentication Servers > New** page. These parameters include:

    - ♦ RADIUS Server IP Address
    - ♦ Shared Secret
    - ♦ Port Number
    - ♦ Server Status

    This document uses the ACS server with an IP address of 10.77.244.196.



3. Click **Apply**.

Configure the WLAN for WPA2 Enterprise Mode of Operation

Next, configure the WLAN which the clients will use to connect to the wireless network. The WLAN SSID for WPA2 enterprise mode will be WPA2−Enterprise. This example assigns this WLAN to the management interface.

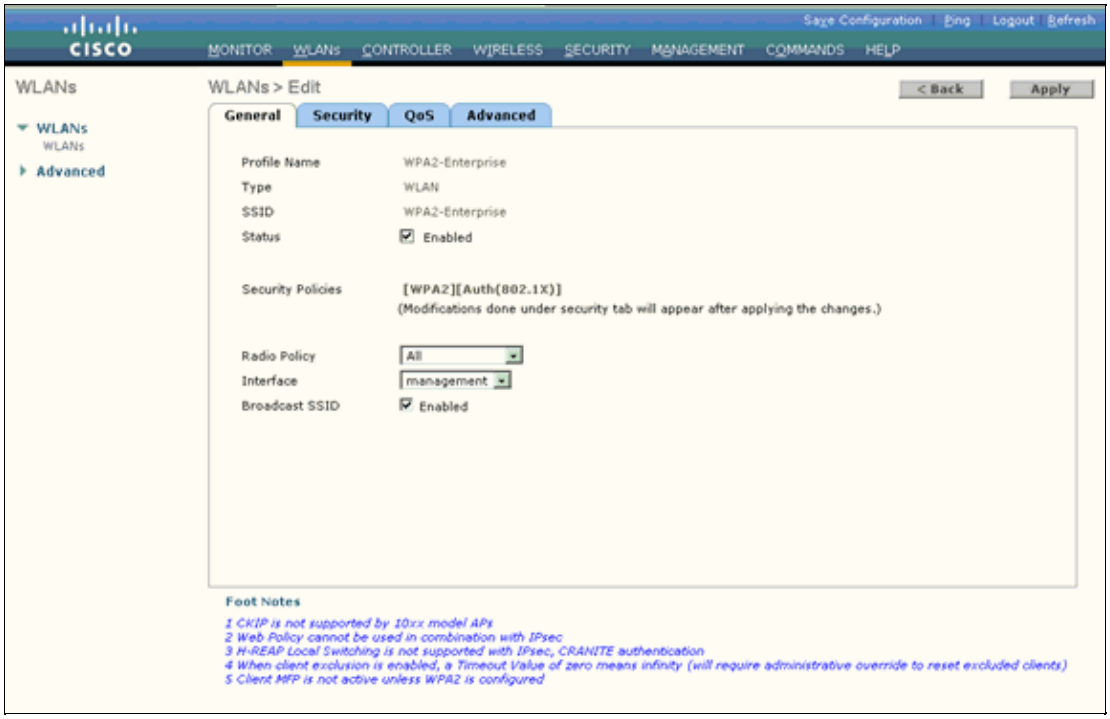
Complete these steps in order to configure the WLAN and its related parameters:

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

   This page lists the WLANs that exist on the controller.
2. Click **New** in order to create a new WLAN.
3. Enter the WLAN SSID name, and the Profile name on the **WLANs > New** page. Then, click **Apply**.

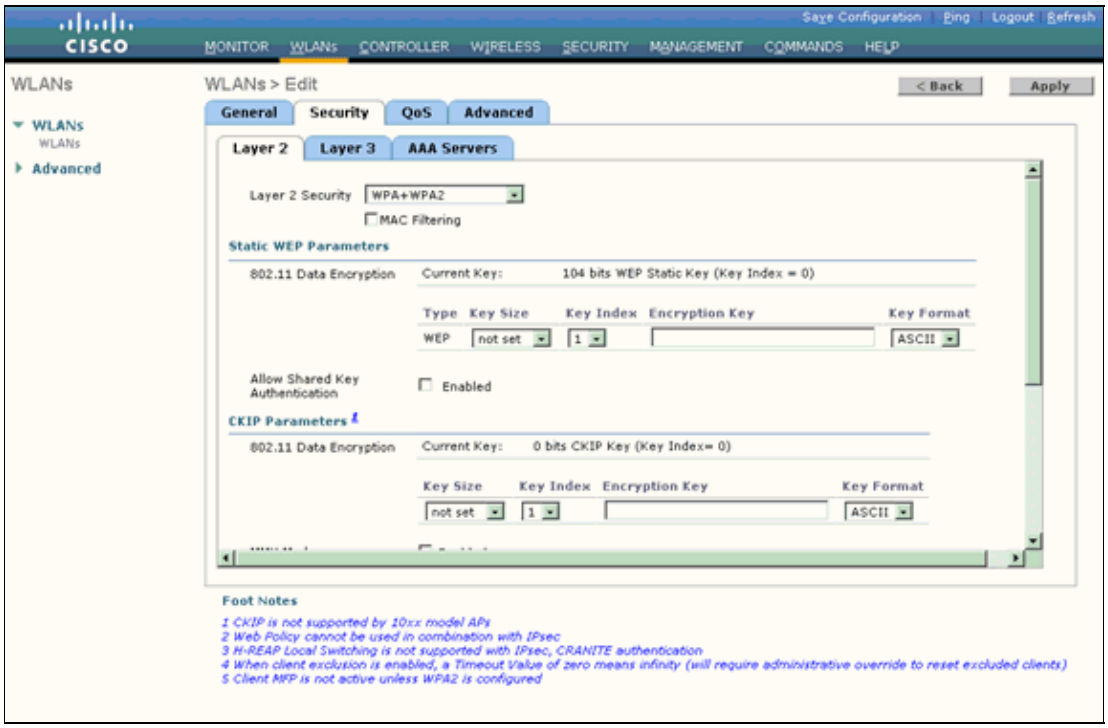
   This example uses **WPA2−Enterprise** as the SSID.

4. Once you create a new WLAN, the **WLAN > Edit** page for the new WLAN appears. On this page, you can define various parameters specific to this WLAN. This includes General Policies, Security Policies, QOS policies and Advanced parameters.
5. Under General Policies, check the **Status** check box in order to enable the WLAN.



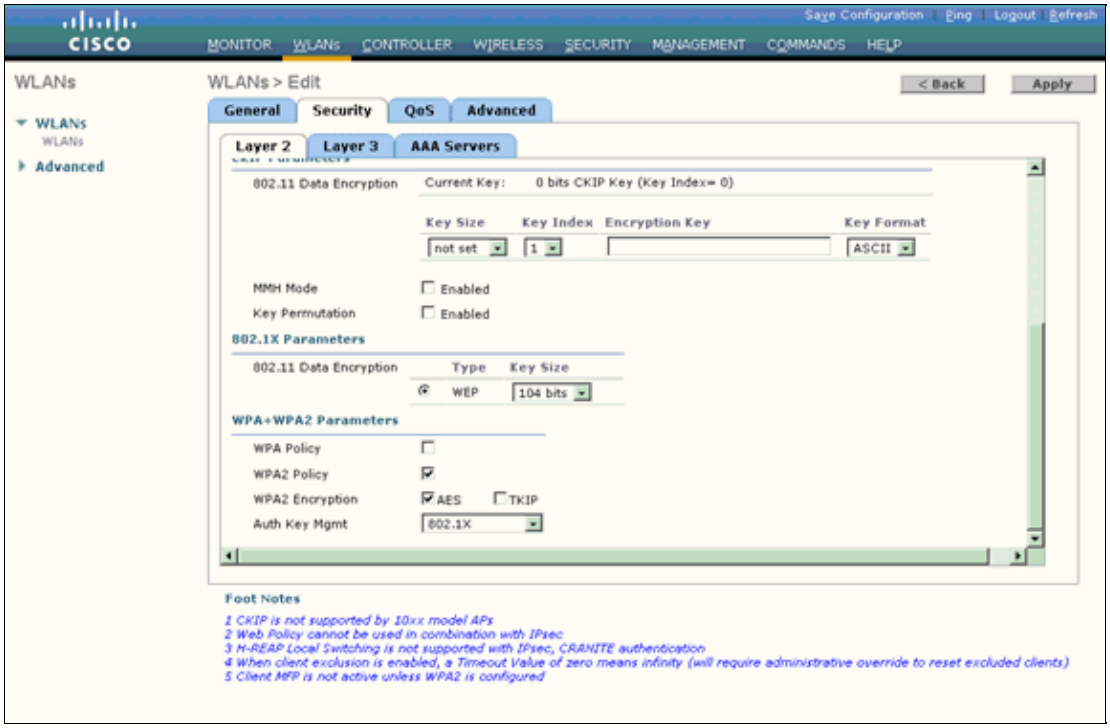
6. If you want the AP to broadcast the SSID in its beacon frames, check the **Broadcast SSID** check box.
7. Click the **Security** tab. Under Layer 2 Security, choose **WPA+WPA2**.

   This enables WPA authentication for the WLAN.



8. Scroll down the page to modify the **WPA+WPA2 Parameters**.

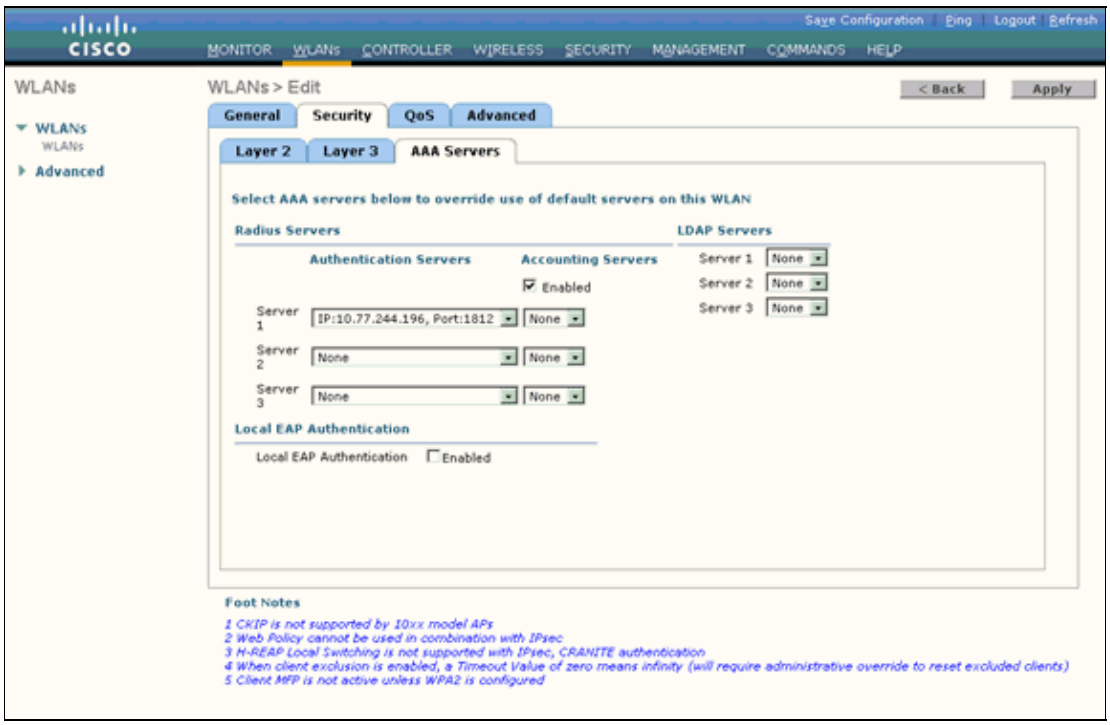
   In this example, WPA2 Policy and AES encryption are selected.



9. Under Auth Key Mgmt, choose **802.1x**.

   This enables WPA2 using 802.1x/EAP authentication and AES encryption for the WLAN.
10. Click the **AAA Servers** tab. Under Authentication Servers, choose the appropriate server IP address.

    In this example, 10.77.244.196 is used as the RADIUS server.



11. Click **Apply**.

    Note: This is the only EAP setting that needs to be configured on the controller for EAP authentication. All other configurations specific to EAP−FAST need to be done on the RADIUS server and the clients that need to be authenticated.

Configure the RADIUS Server for WPA2 Enterprise Mode Authentication (EAP−FAST)

In this example, Cisco Secure ACS is used as the external RADIUS server. Perform these steps in order to configure the RADIUS server for EAP−FAST authentication:

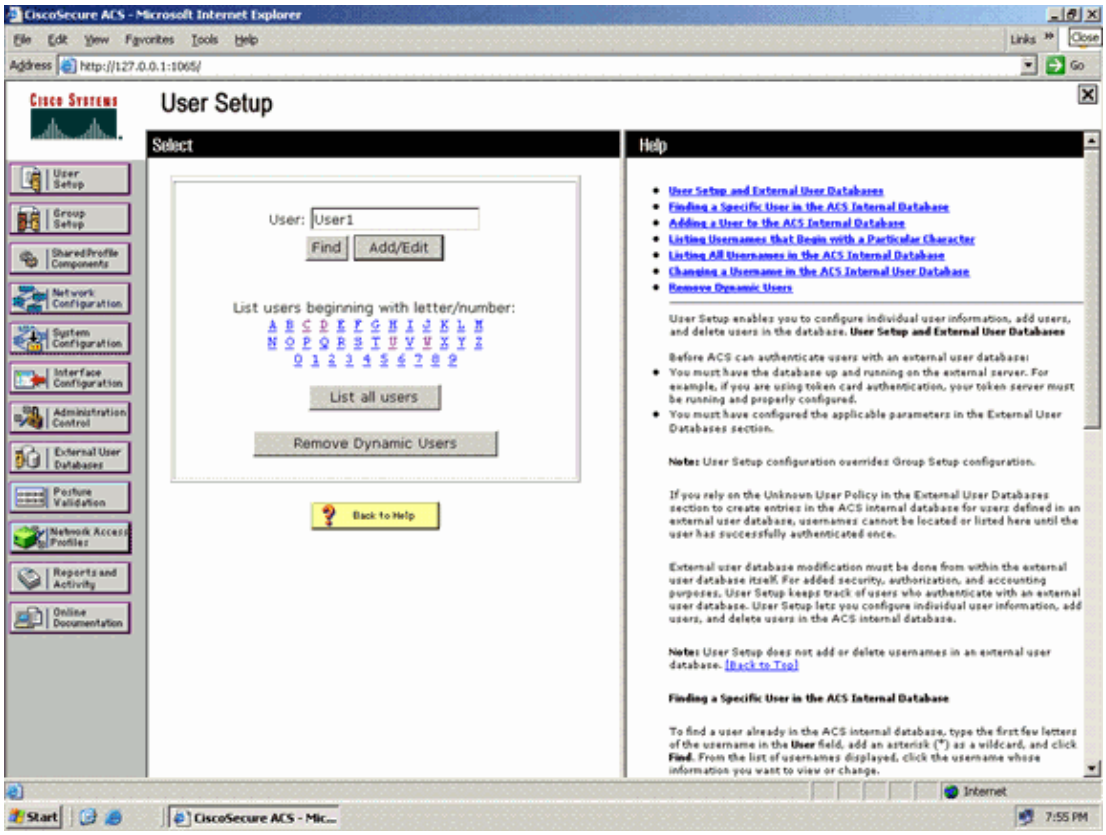
1. Create a User Database to Authenticate Clients
2. Add the WLC as AAA Client to the RADIUS Server
3. Configure EAP−FAST Authentication on the RADIUS Server with Anonymous In−band PAC Provisioning

   Note: EAP−FAST can be configured either with Anonymous In−band PAC Provisioning or Authenticated In−band PAC Provisioning. This example uses Anonymous In−band PAC Provisioning. For detailed information and examples on configuring EAP FAST with Anonymous In−band PAC Provisioning and Authenticated In−band Provisioning, refer to EAP−FAST Authentication with Wireless LAN Controllers and External RADIUS Server Configuration Example.

Create a User Database to Authenticate EAP−FAST Clients

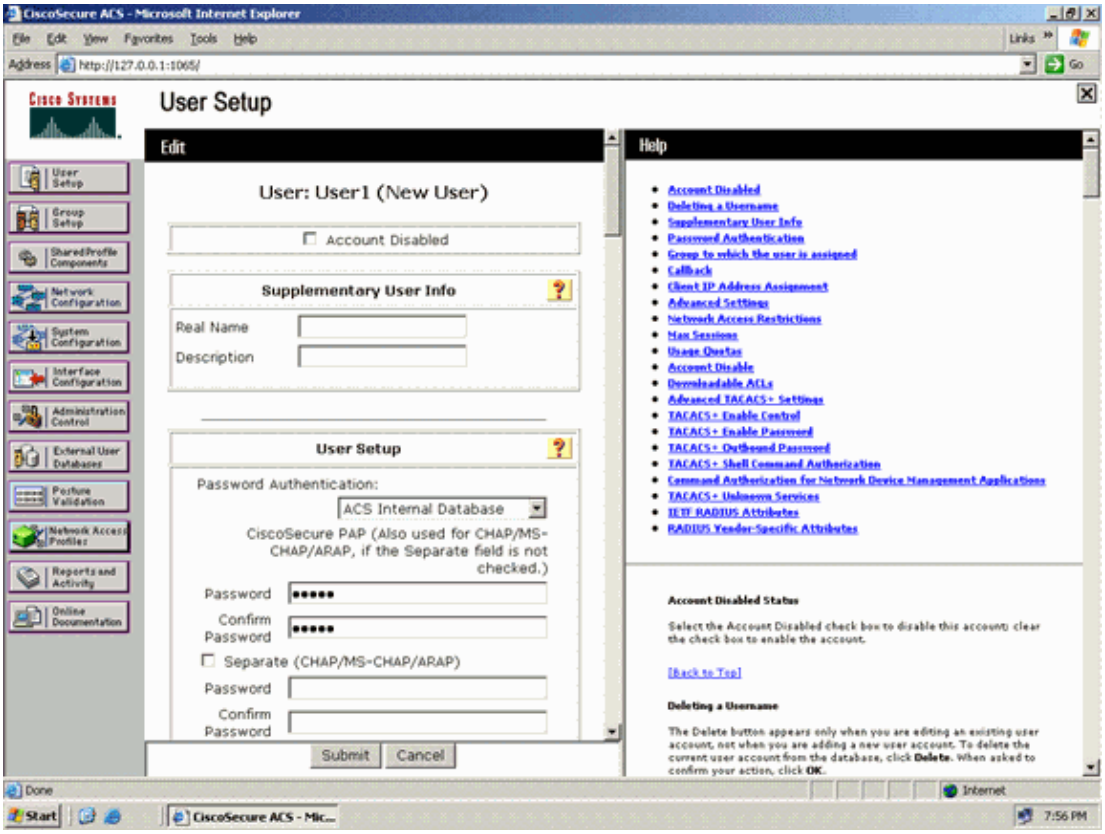
Complete these steps in order to create a user database for EAP−FAST clients on the ACS. This example configures username and password of the EAP−FAST client as User1 and User1, respectively.

1. From the ACS GUI in the navigation bar, select **User Setup**. Create a new user wireless, and then click **Add/Edit** in order to go to the Edit page of this user.



2. From the User Setup Edit page, configure Real Name and Description as well as the Password settings as shown in this example.

   This document uses **ACS Internal Database** for Password Authentication.

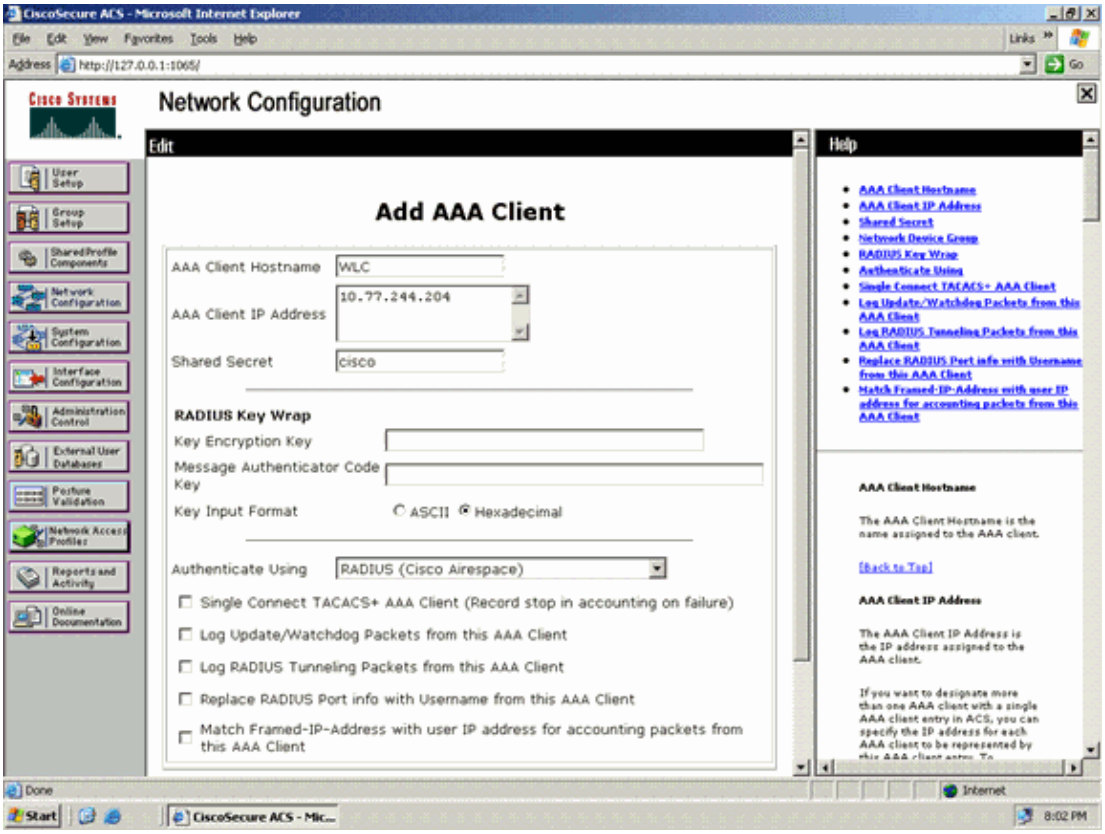


3. Choose **ACS Internal Database** from the Password Authentication drop−down box.
4. Configure all the other required parameters and click **Submit**.

Add the WLC as AAA Client to the RADIUS Server

Complete these steps in order to define the controller as an AAA client on the ACS server:

1. Click **Network Configuration** from the ACS GUI. Under the Add AAA client section of the Network Configuration page, click **Add Entry** in order to add the WLC as the AAA client to the RADIUS server.
2. From the AAA Client page, 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.

3. Click **Submit+Apply**.

Configure EAP−FAST Authentication on the RADIUS Server with Anonymous In−band PAC Provisioning

Anonymous In−band Provisioning

This is one of the two in−band provisioning methods in which the ACS establishes a secured connection with the end−user client for the purpose of providing the client with a new PAC. This option allows an anonymous TLS handshake between the end−user client and ACS.

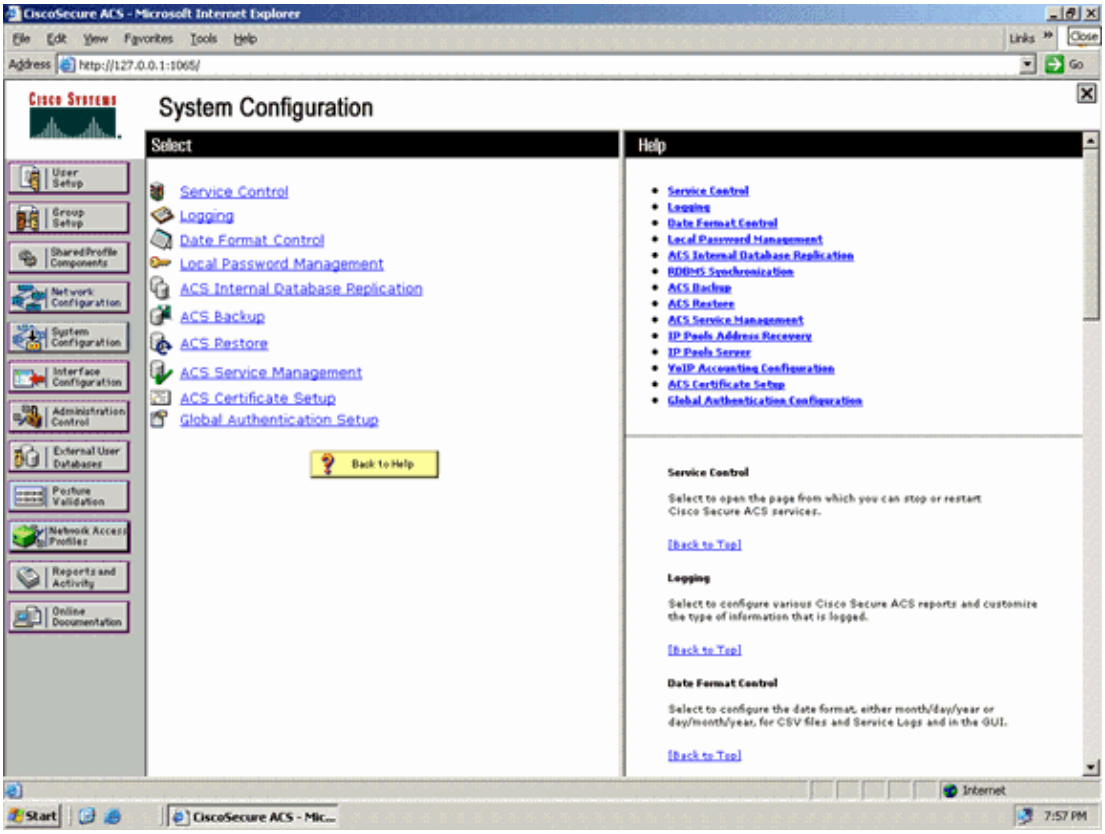
This method operates inside an Authenticated Diffie−HellmanKey Agreement Protocol (ADHP) tunnel before the peer authenticates the ACS server.

Then, the ACS requires EAP−MS−CHAPv2 authentication of the user. At successful user authentication, the ACS establishes a Diffie−Hellman tunnel with the end−user client. The ACS generates a PAC for the user and sends it to the end−user client in this tunnel, along with information about this ACS. This method of provisioning uses EAP−MSCHAPv2 as the authentication method in phase zero and EAP−GTC in phase two.

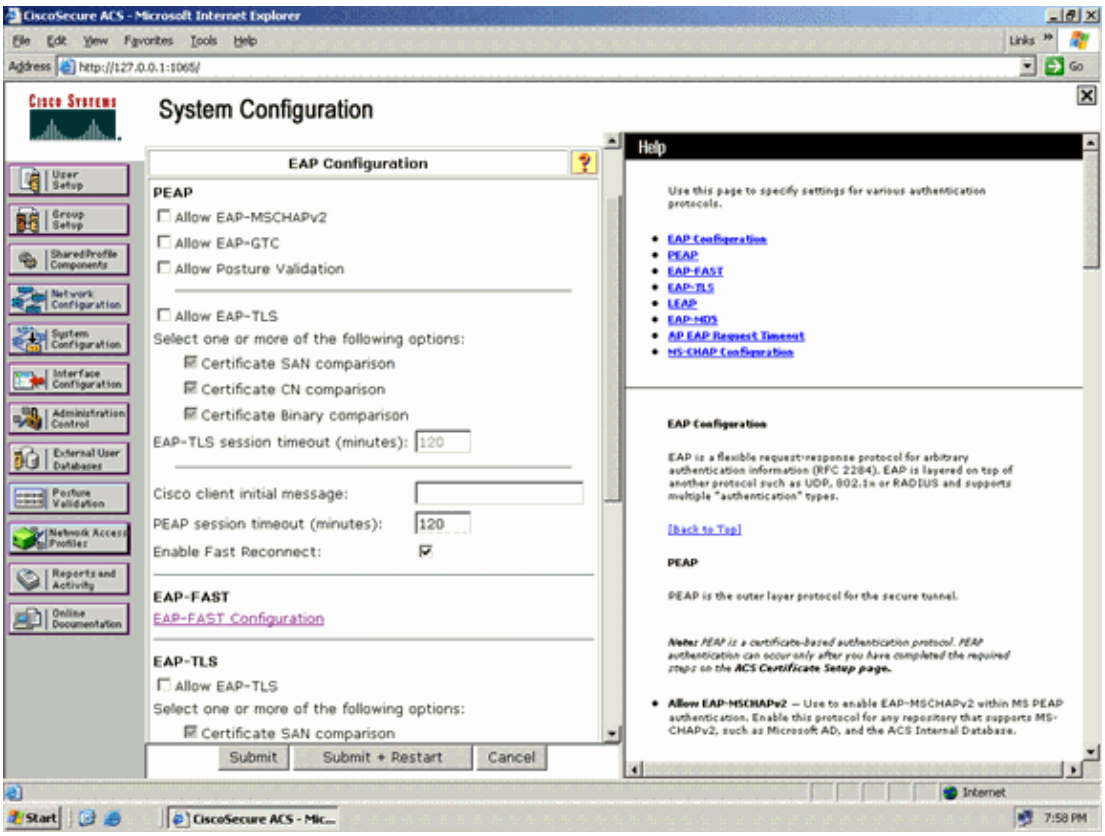
Because an unauthenticated server is provisioned, it is not possible to use a plain text password. Therefore, only MS−CHAP credentials can be used inside the tunnel. MS−CHAPv2 is used to prove the peer's identity and receive a PAC for further authentication sessions (EAP−MS−CHAP will be used as inner method only).

Complete these steps in order to configure EAP−FAST authentication in the RADIUS server for anonymous in−band provisioning:

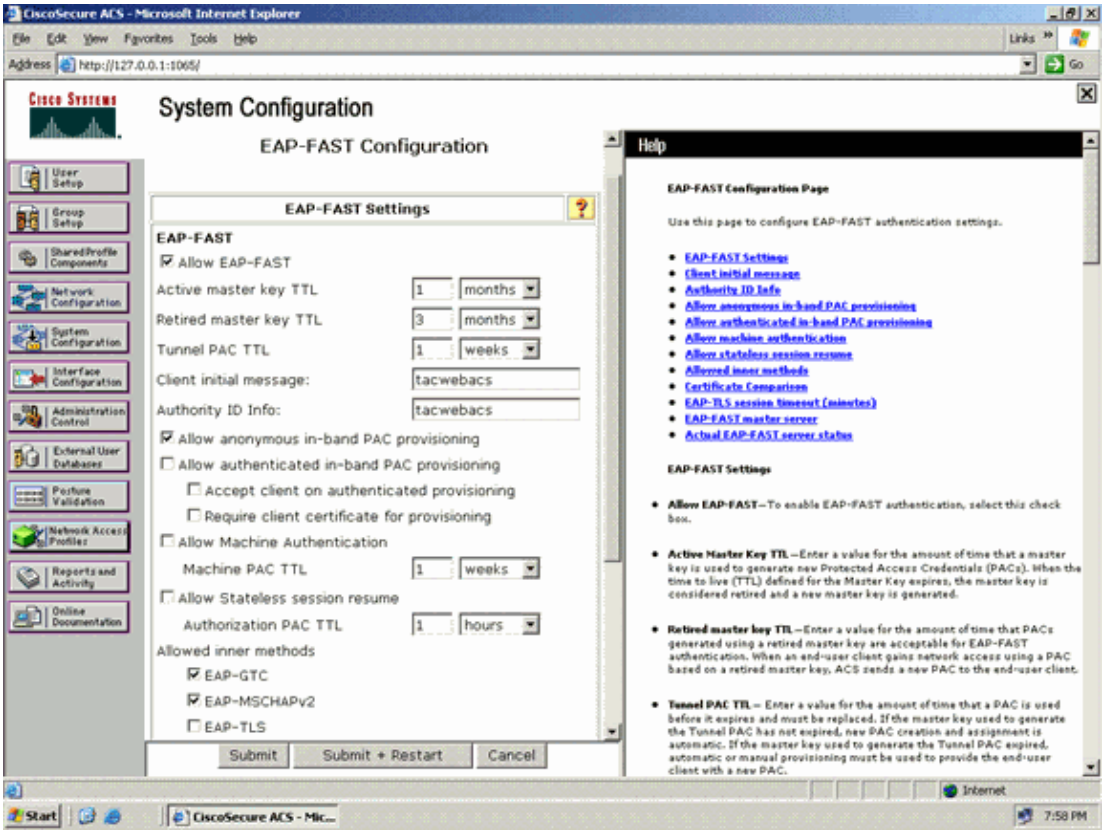
1. Click **System Configuration** from the RADIUS server GUI. From the System Configuration page, choose **Global Authentication Setup**.



2. From the Global Authentication setup page, click **EAP−FAST Configuration** in order to go to the EAP−FAST settings page.



3. From the EAP−FAST Settings page, check the **Allow EAP−FAST** check box to enable EAP−FAST in the RADIUS server.



4. Configure the Active/Retired master key TTL (Time−to−Live) values as desired, or set it to the default value as shown in this example.

   Refer to Master Keys for information about Active and Retired master keys. Also, refer to Master Keys and PAC TTLs for more information.

   The Authority ID Info field represents the textual identity of this ACS server, which an end user can use to determine which ACS server to be authenticated against. Filling in this field is mandatory.

   The Client initial display message field specifies a message to be sent to users who authenticate with an EAP−FAST client. Maximum length is 40 characters. A user will see the initial message only if the end−user client supports the display.
5. If you want the ACS to perform anonymous in−band PAC provisioning, check the **Allow anonymous in−band PAC provisioning** check box.
6. **Allowed inner methods** "This option determines which inner EAP methods can run inside the EAP−FAST TLS tunnel. For anonymous in−band provisioning, you must enable EAP−GTC and EAP−MS−CHAP for backward compatibility. If you select Allow anonymous in−band PAC provisioning, you must select EAP−MS−CHAP (phase zero) and EAP−GTC (phase two).

Configure the Wireless Client for WPA2 Enterprise Mode of Operation

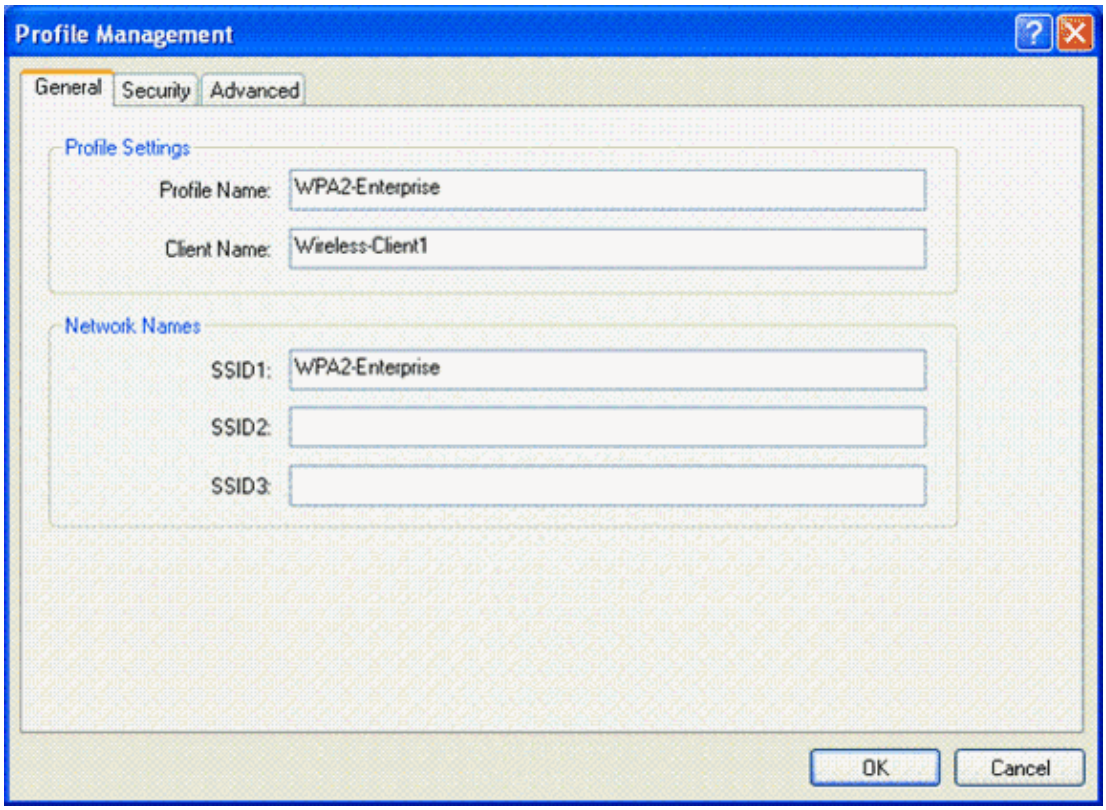
The next step is to configure the wireless client for WPA2 Enterprise mode of operation.

Complete these steps in order to configure the wireless client for WPA2 Enterprise mode.

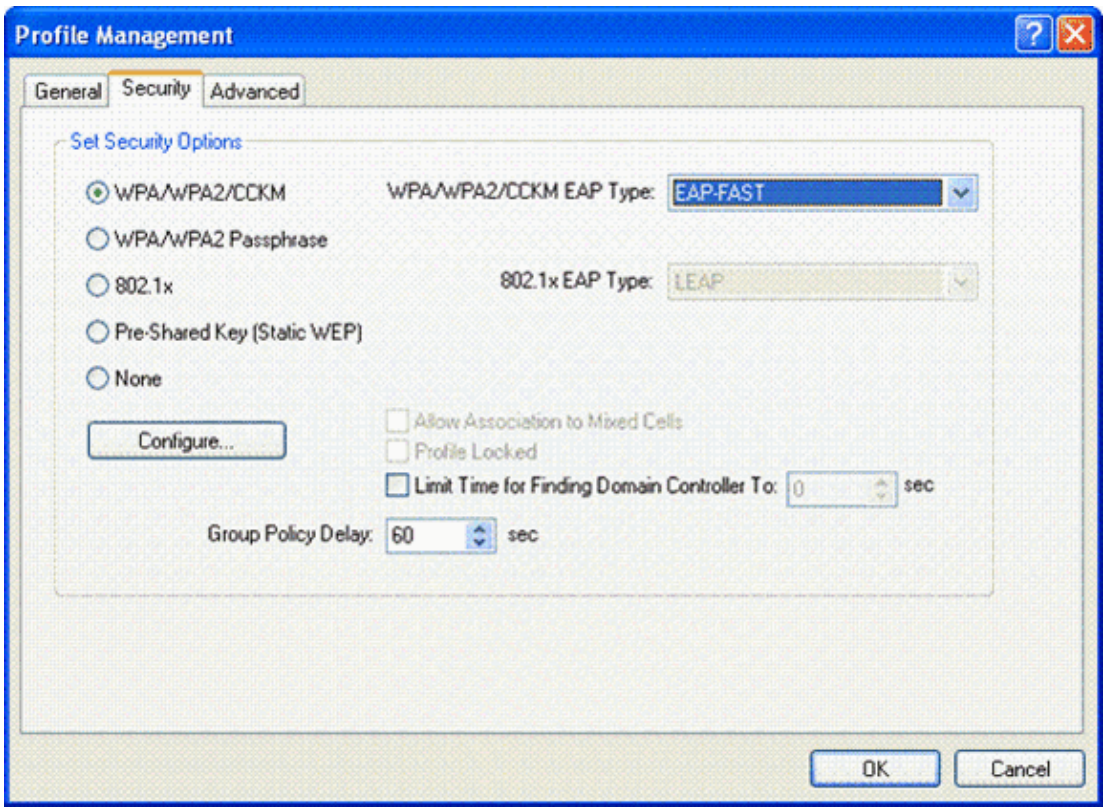
1. From the Aironet Desktop Utility window, click **Profile Management > New** in order to create a profile for the WPA2−Enterprise WLAN user.

   As mentioned earlier, this document uses the WLAN/SSID name as **WPA2−Enterprise** for the wireless client.

2. From the Profile Management window, click the **General** tab and configure the Profile Name, Client Name and SSID name as shown in this example. Then, click **OK**

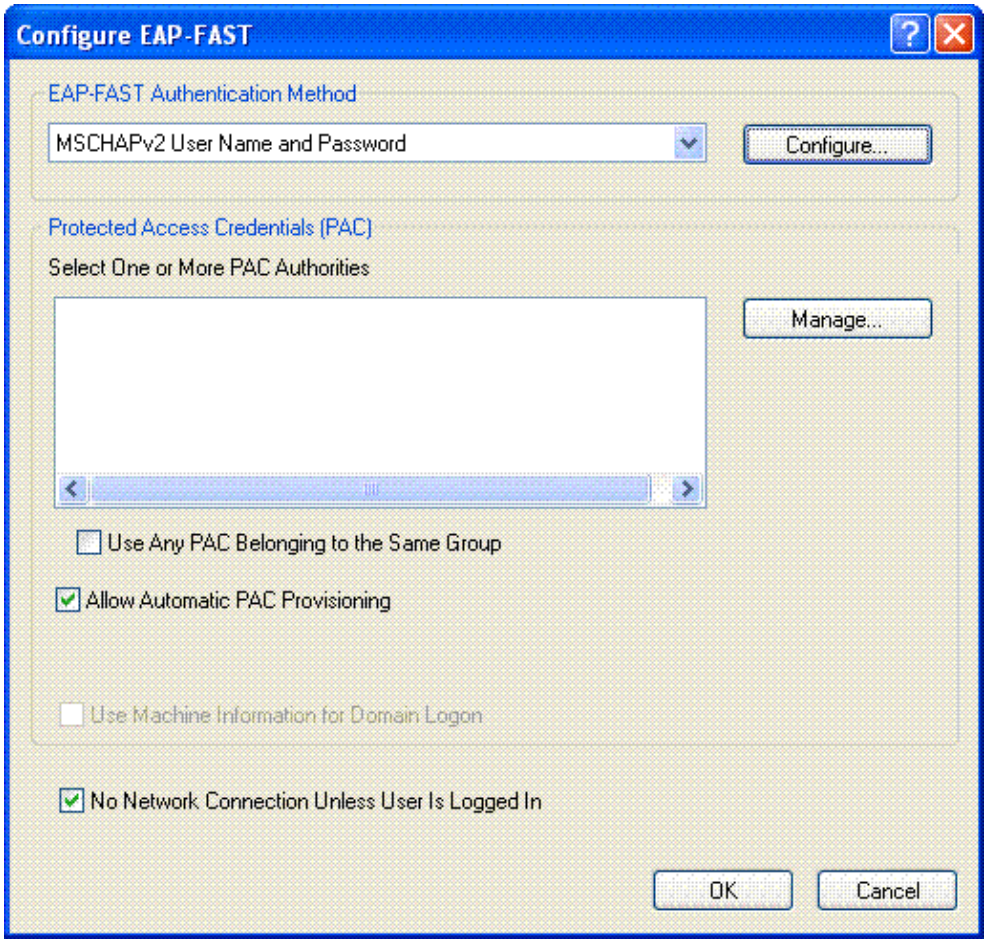


3. Click the **Security** tab and choose **WPA/WPA2/CCKM** to enable WPA2 mode of operation. Under WPA/WPA2/CCKM EAP Type, choose **EAP−FAST**. Click **Configure** in order to configure the EAP−FAST setting.



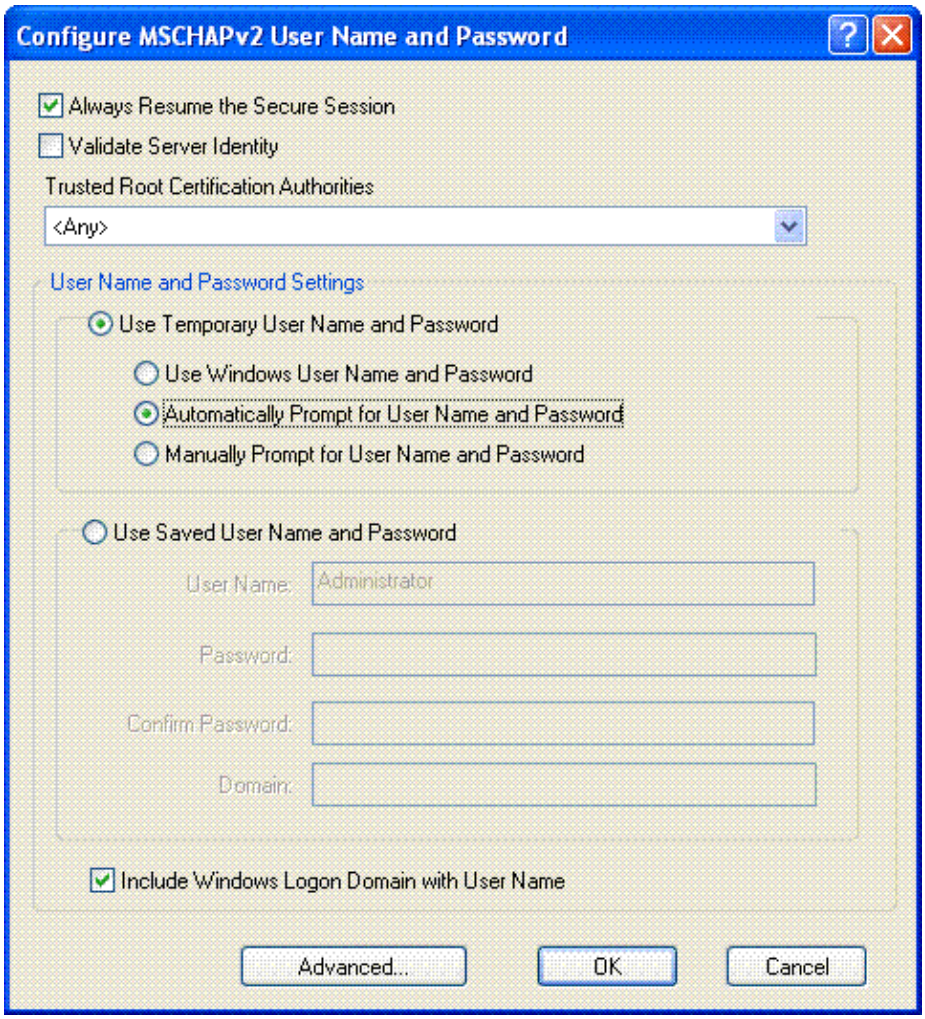
4. From the Configure EAP−FAST window, check the **Allow Automatic PAC Provisioning** check box. If you want to configure anonymous PAC provisioning, EAP−MS−CHAP will be used as the only

inner method in phase zero.



5. Choose MSCHAPv2 User Name and Password as the authentication method from the EAP−FAST Authentication Method drop−down box. Click **Configure**.
6. From the Configure MSCHAPv2 User Name and Password window, choose the appropriate username and password settings.

   This example chooses **Automatically Prompt for User Name and Password**.



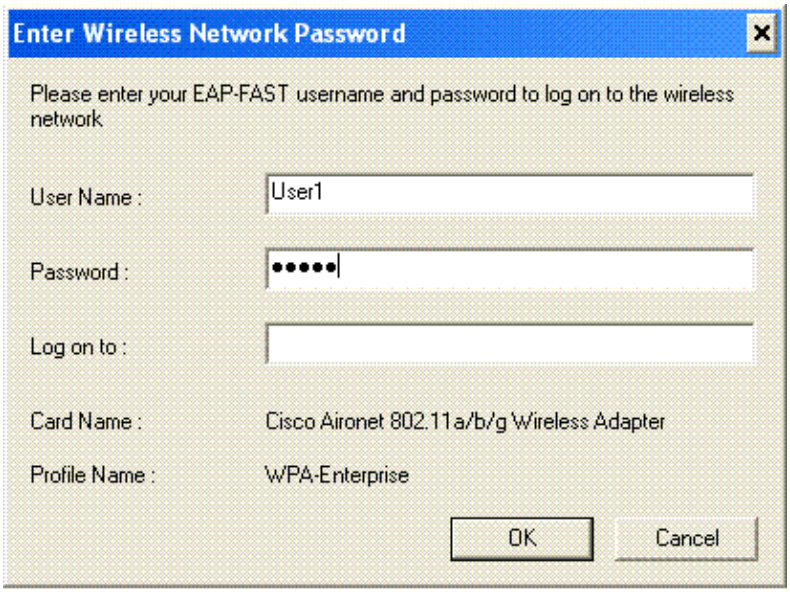
The same username and password should be registered at the ACS. As mentioned earlier, this example uses User1 and User1 respectively as the username and password. Also, note that this is an anonymous in−band provisioning. Therefore, the client cannot validate the server certificate. You need to make sure that the Validate Server Identity check box is unchecked.

7. Click **OK**.

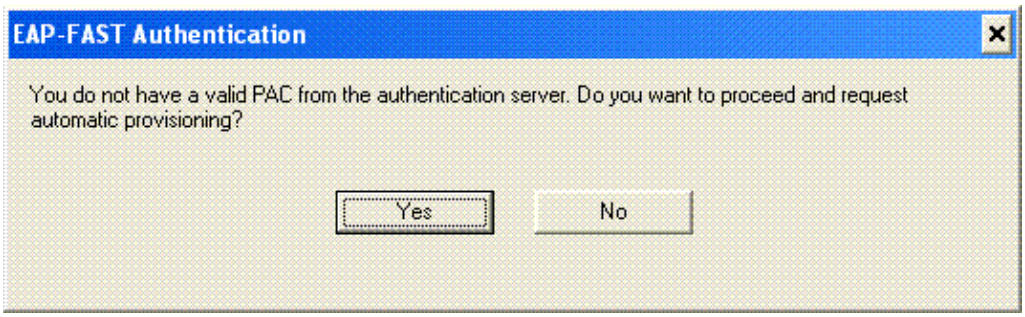
Verify WPA2 Enterprise Mode of Operation

Complete these steps in order to verify whether your WPA2 Enterprise mode configuration works properly:

1. From the Aironet Desktop Utility window, select the profile **WPA2−Enterprise** and click **Activate** in order to activate the wireless client profile.
2. If you have enabled MS−CHAP ver2 as your authentication, then the client will prompt for the username and password.

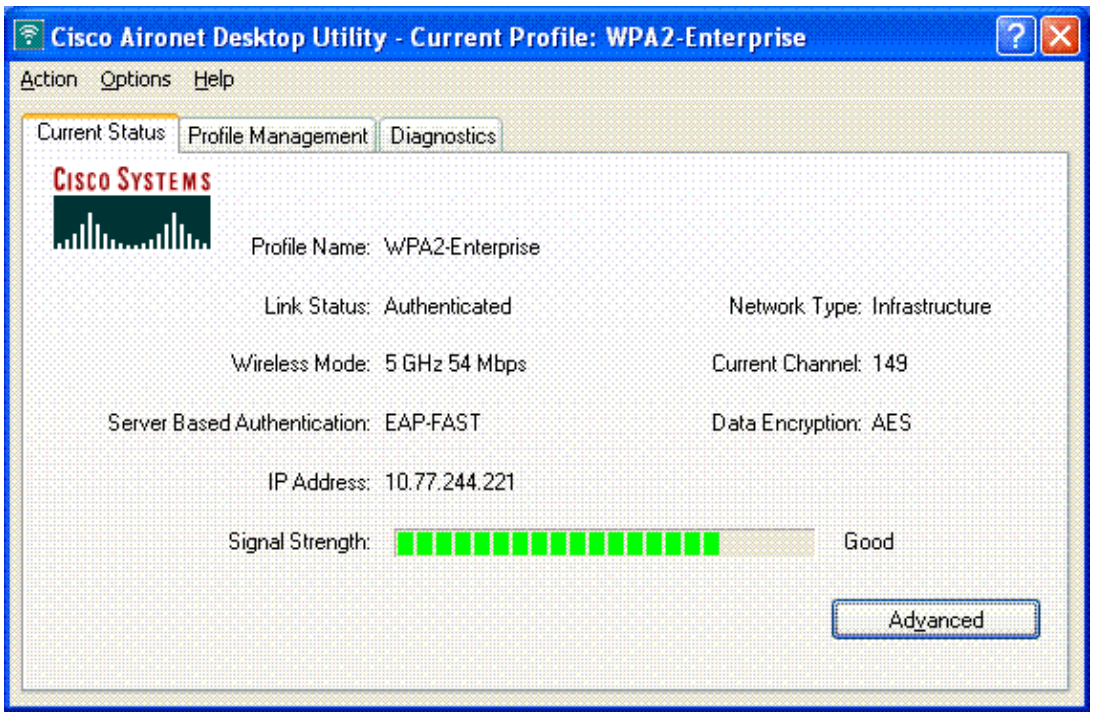


3. During EAP−FAST processing of the user, you will be prompted by the client to request PAC from the RADIUS server. When you click **Yes**, PAC provisioning starts.



4. After successful PAC provisioning in phase zero, phase one and two follow and a successful authentication procedure takes place.

   Upon successful authentication the wireless client gets associated to the WLAN WPA2−Enterprise. Here is the screenshot:



You can also verify whether the RADIUS server receives and validates the authentication request from the wireless client. 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.

Configure the Devices for WPA2 Personal Mode

Perform these steps in order to configure the devices for WPA2−Personal mode of operation:

1. Configure the WLAN for WPA2 Personal Mode Authentication
2. Configure the Wireless Client for WPA2 Personal Mode

Configure the WLAN for WPA2 Personal Mode of Operation

You need to configure the WLAN which the clients will use to connect to the wireless network. The WLAN SSID for WPA2 Personal mode will be WPA2−Personal. This example assigns this WLAN to the management interface.

Complete these steps in order to configure the WLAN and its related parameters:

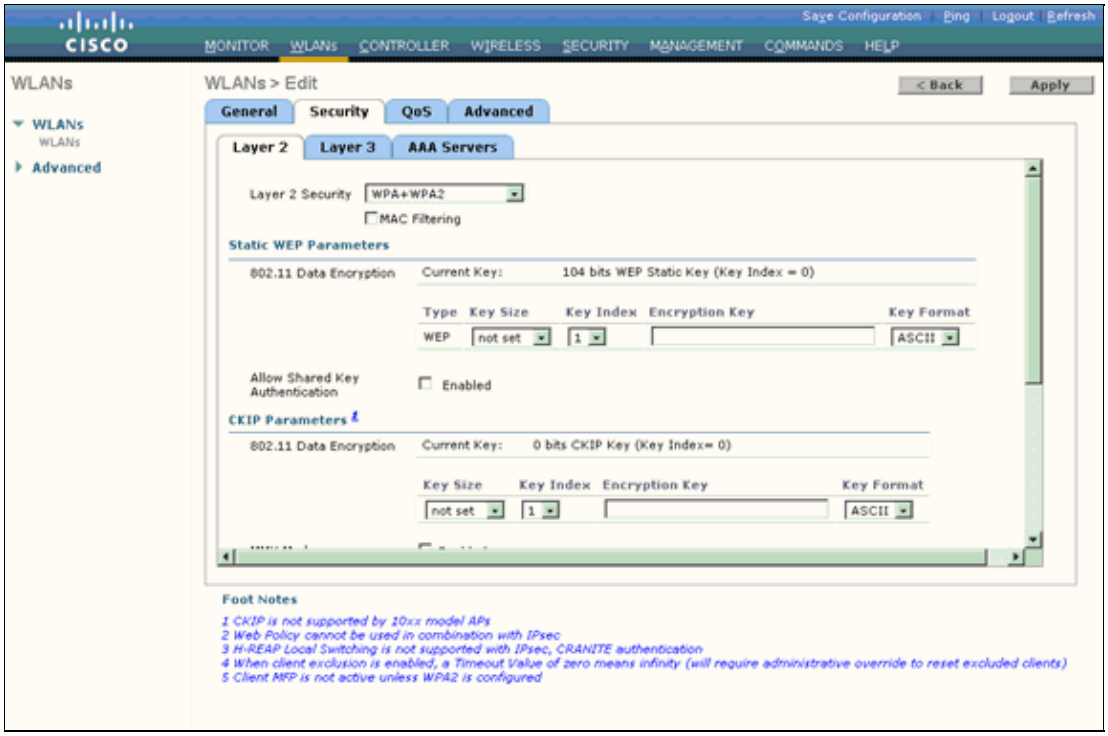
1. Click **WLANs** from the GUI of the controller in order to display the WLANs page.

   This page lists the WLANs that exist on the controller.
2. Click **New** in order to create a new WLAN.
3. Enter the WLAN SSID name, Profile name and WLAN ID on the WLANs > New page. Then, click **Apply**.

   This example uses **WPA2−Personal** as the SSID.

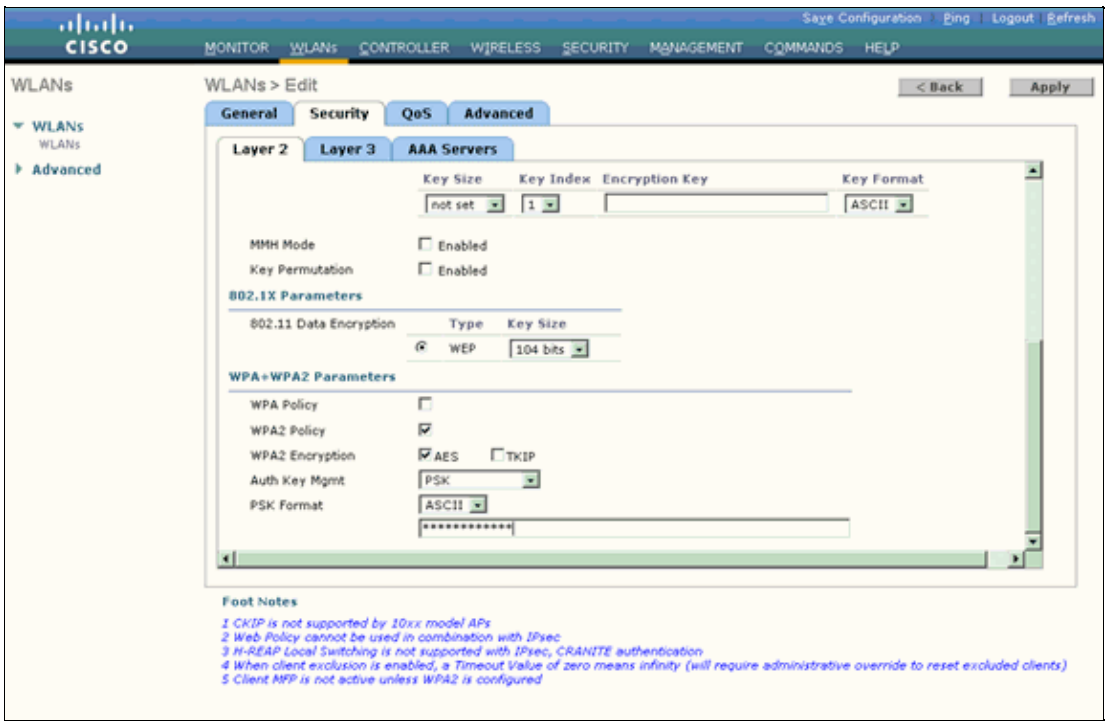
4. Once you create a new WLAN, the **WLAN > Edit** page for the new WLAN appears. On this page, you can define various parameters specific to this WLAN. This includes General Policies, Security Policies, QOS policies and Advanced parameters.
5. Under General Policies, check the **Status** check box in order to enable the WLAN.
6. If you want the AP to broadcast the SSID in its beacon frames, check the **Broadcast SSID** check box.
7. Click the **Security** tab. Under Layer Security, choose **WPA+WPA2**.

   This enables WPA authentication for the WLAN.



8. Scroll down the page to modify the **WPA+WPA2 Parameters**.

   In this example, WPA2 Policy and AES encryption are selected.
9. Under Auth Key Mgmt, choose **PSK** in order to enable WPA2−PSK.
10. Enter the pre−shared key in the appropriate field as shown.



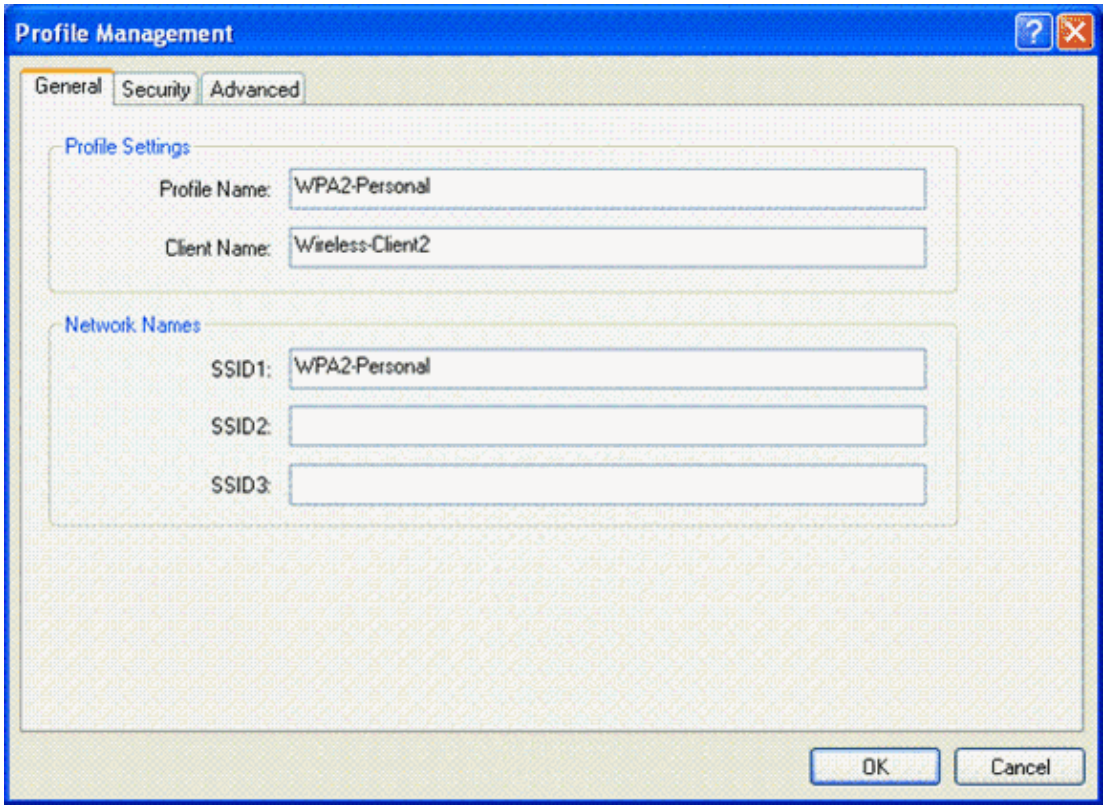
   Note: Pre−shared Key used on the WLC must match with the one configured on the wireless clients.
11. Click **Apply**.

Configure the Wireless Client for WPA2 Personal Mode

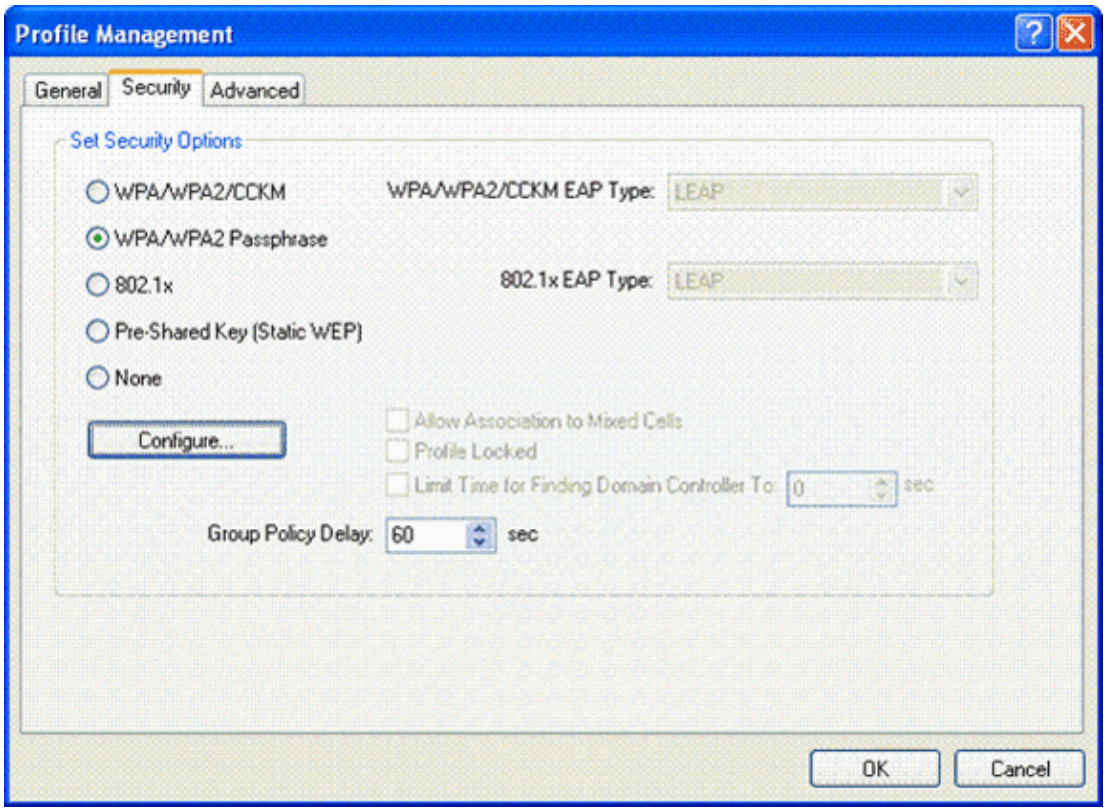
The next step is to configure the wireless client for WPA2−Personal mode of operation.

Complete these steps in order to configure the wireless client for WPA2−Personal mode:

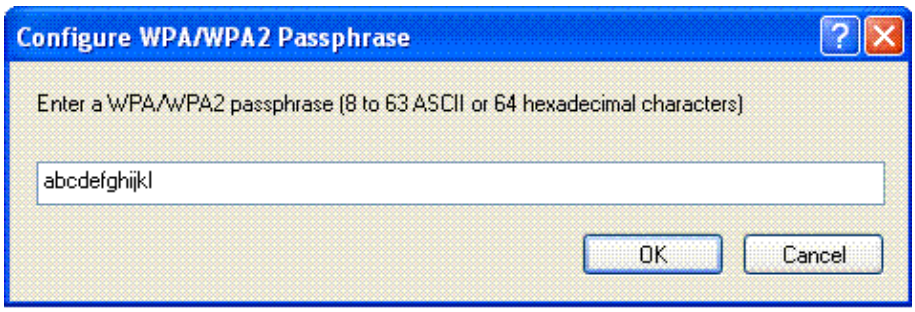
1. From the Aironet Desktop Utility window, click **Profile Management > New** in order to create a profile for WPA2−PSK WLAN user.
2. From the Profile Management window, click the **General** tab and configure the Profile Name, Client Name and SSID name as shown in this example. Then, click **OK**.



3. Click the **Security** tab and choose **WPA/WPA2 Passphrase** to enable WPA2−PSK mode of operation. Click **Configure** in order to configure the WPA−PSK pre−shared key.



4. Enter the preshared key and click **OK**.

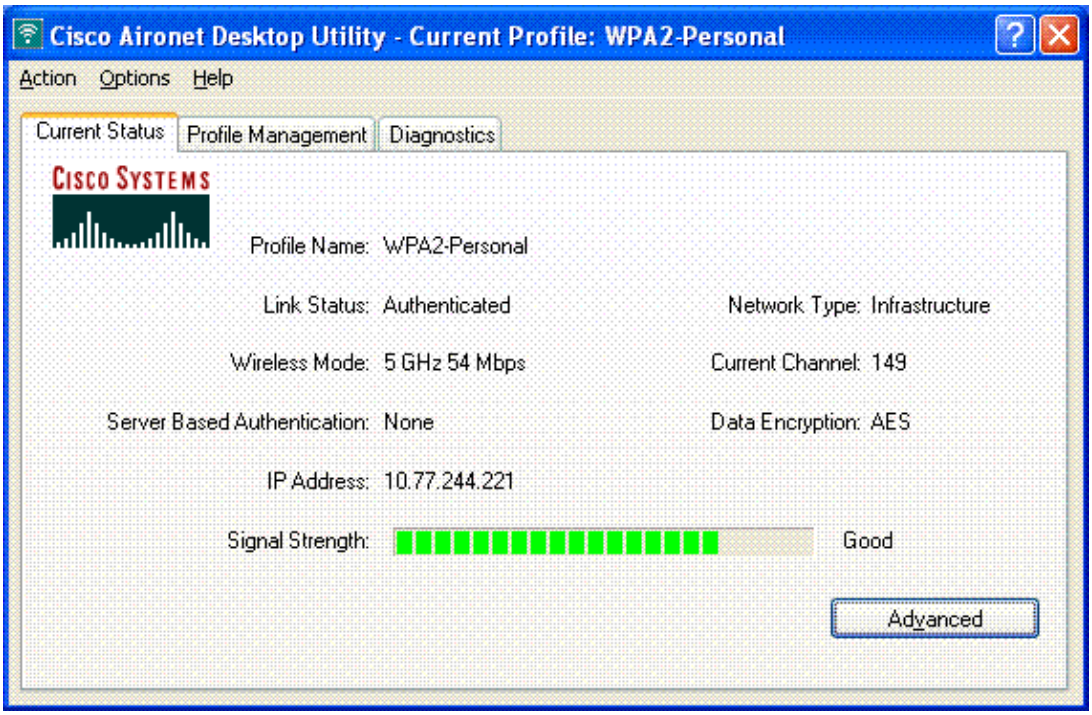


Verify WPA2−Personal Mode of Operation

Complete these steps in order to verify whether your WPA2−Enterprise mode configuration works properly:

1. From the Aironet Desktop Utility window, select the profile **WPA2−Personal** and click **Activate** in order to activate the wireless client profile.
2. Once the profile is activated, the wireless client associates to the WLAN upon successful authentication.

   Here is the screenshot:



Troubleshoot

This section provides information you can use to troubleshoot your configuration.

These **debug** commands will be useful for troubleshooting the configuration:

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

- **debug dot1x events enable** "Enables the debug of all dot1x events. Here is an example debug output based on successful authentication:

  Note: Some of the lines from this output have been moved to second lines due to space limitations.

```
(Cisco Controller)>debug dot1x events enable
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP -Request/Identity
to mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAPOL START from
mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity
to mobile 00:40:96:af:3e:93 (EAP Id 2)
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAP Response packet with
mismatching id (currentid=2, eapid=1) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received Identity Response
(count=2) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Processing Access-Challenge
for mobile 00:40:96:af:3e:93
.....................................................................
.....................................................................
.....................................................................
.....................................................................

Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 43)
Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Processing Access-Challenge
for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA
to mobile 00:40:96:af:3e:93 (EAP Id 20)
```

```
Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)
Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 −0
Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3689 seconds on
AP 00:0b:85:91:c3:c0
Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 −1
Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3696 seconds on
AP 00:0b:85:91:c3:c0
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP−Request/Identity to
mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3)
from mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access−Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING: updated EAP−Identifer 22 ===>
19 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 19)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 3)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access−Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 20)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access−Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 21)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access−Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access−Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 23)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 23, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access−Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 24)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access−Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 25)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access−Challenge for
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to
mobile 00:40:96:af:3e:93 (EAP Id 26)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from
mobile 00:40:96:af:3e:93 (EAP Id 26, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access−Challenge for
mobile 00:40:96:af:3e:93
```

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 27)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 27, EAP Type 43)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access−Reject for mobile00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP−Failure to mobile 00:4096:af:3e:93 (EAP Id 27)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Setting quiet timer for 5 seconds for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP−Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP−Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1)
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP−Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Identity Response (count=2) from mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access−Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP−Identifer 2 ===> 20 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 3)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access−Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access−Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access−Challenge for mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP−Identifer 22 ===> 24 for STA 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Processing Access−Challenge for mobile 00:40:96:af:3e:93**
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25)**
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43)**
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Processing Access−Accept for mobile 00:40:96:af:3e:93**
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Creating a new PMK Cache Entry for tation 00:40:96:af:3e:93 (RSN 0)**
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending EAP−Success to mobile 00:40:96:af:3e:93 (EAP Id 25)**
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending default RC4 key to mobile 00:40:96:af:3e:93**
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending Key−Mapping RC4 key to mobile 00:40:96:af:3e:93**
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Received Auth Success while in Authenticating state for mobile 00:40:96:af:3e:93**

- **debug dot1x packet enable** "Enables the debug of 802.1x packet messages.
- **debug aaa events enable** "Enables the debug output of all aaa events.

Related Information

- **WPA2 − Wi−Fi Protected Access 2**
- **EAP−FAST Authentication with Wireless LAN Controllers and External RADIUS Server Configuration Example**
- **EAP Authentication with WLAN Controllers (WLC) Configuration Example**
- **WPA Configuration Overview**
- **Wireless Product Support**
- **Technical Support & Documentation − Cisco Systems**

Updated: Feb 26, 2008 Document ID: 100708