

# Esempio di configurazione di Wi-Fi Protected Access (WPA) in una rete wireless unificata Cisco

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Supporto WPA e WPA2](#)

[Installazione della rete](#)

[Configurare i dispositivi per la modalità WPA2 Enterprise](#)

[Configurazione del WLC per l'autenticazione RADIUS tramite un server RADIUS esterno](#)

[Configurazione della WLAN per la modalità operativa WPA2 Enterprise](#)

[Configurare il server RADIUS per l'autenticazione in modalità Enterprise WPA2 \(EAP-FAST\)](#)

[Configurazione del client wireless per la modalità di funzionamento WPA2 Enterprise](#)

[Configurare i dispositivi per la modalità personale WPA2](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

## Introduzione

Questo documento descrive come configurare Wi-Fi Protected Access (WPA) in una rete wireless unificata Cisco.

## Prerequisiti

### Requisiti

Prima di provare la configurazione, accertarsi di avere una conoscenza di base di questi argomenti:

- WPA
- Soluzioni per la sicurezza di reti LAN wireless (WLAN)**Nota:** per informazioni sulle soluzioni di sicurezza Cisco WLAN, consultare la [panoramica](#) della [sicurezza](#) Cisco [Wireless LAN](#).

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 1000 Lightweight Access Point (LAP)
- Cisco Wireless LAN Controller (WLC) 4404 con firmware 4.2.61.0
- Cisco 802.11a/b/g client adapter con firmware 4.1
- Aironet Desktop Utility (ADU) con firmware 4.1
- Cisco Secure ACS server versione 4.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Convenzioni

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

## Supporto WPA e WPA2

Cisco Unified Wireless Network include il supporto per le certificazioni Wi-Fi Alliance WPA e WPA2. WPA è stato introdotto dalla Wi-Fi Alliance nel 2003. WPA2 è stato introdotto dalla Wi-Fi Alliance nel 2004. Tutti i prodotti con certificazione Wi-Fi per WPA2 devono essere interoperabili con i prodotti con certificazione Wi-Fi per WPA.

WPA e WPA2 offrono agli utenti finali e agli amministratori di rete un elevato livello di garanzia che i loro dati rimarranno privati e che l'accesso alle loro reti sarà limitato agli utenti autorizzati. Entrambe hanno modalità operative personali ed aziendali che soddisfano le esigenze specifiche dei due segmenti di mercato. La modalità Enterprise di ciascun sistema utilizza IEEE 802.1X ed EAP per l'autenticazione. La modalità personale di ciascuna utilizza la chiave già condivisa (PSK) per l'autenticazione. Cisco sconsiglia la modalità personale per le distribuzioni aziendali o governative, in quanto utilizza una chiave PSK per l'autenticazione utente. PSK non è sicuro per gli ambienti aziendali.

WPA risolve tutte le vulnerabilità WEP conosciute nell'implementazione di sicurezza IEEE 802.11 originale, offrendo una soluzione di sicurezza immediata per le WLAN sia negli ambienti aziendali che in quelli dei piccoli uffici o degli uffici domestici (SOHO). WPA utilizza TKIP per la crittografia.

WPA2 è la nuova generazione di protezione Wi-Fi. È l'implementazione interoperabile dello standard IEEE 802.11i ratificato da parte della Wi-Fi Alliance. Implementa l'algoritmo di crittografia AES consigliato dal National Institute of Standards and Technology (NIST) utilizzando la modalità Counter con il protocollo CCMP (Cipher Block Chaining Message Authentication Code Protocol). WPA2 semplifica la conformità FIPS 140-2 della pubblica amministrazione.

### Confronto tra tipi di modalità WPA e WPA2

	WPA	WPA2
<b>Modalità Enterprise (Business, Government, Education)</b>	<ul style="list-style-type: none"><li>• Autenticazione: IEEE 802.1X/EAP</li></ul>	<ul style="list-style-type: none"><li>• Autenticazione: IEEE 802.1X/EAP</li></ul>

	<ul style="list-style-type: none"> <li>• Crittografia : TKIP/MIC</li> </ul>	<ul style="list-style-type: none"> <li>• Crittografia: AES-CCMP</li> </ul>
<b>Modalità personale (SOHO, Home/Personale)</b>	<ul style="list-style-type: none"> <li>• Autenticazione: PSK</li> <li>• Crittografia : TKIP/MIC</li> </ul>	<ul style="list-style-type: none"> <li>• Autenticazione: PSK</li> <li>• Crittografia: AES-CCMP</li> </ul>

In modalità Enterprise, sia WPA che WPA2 utilizzano 802.1X/EAP per l'autenticazione. 802.1X fornisce alle WLAN un'autenticazione forte e reciproca tra un client e un server di autenticazione. Inoltre, 802.1X fornisce chiavi di crittografia dinamiche per utente e per sessione, rimuovendo il carico amministrativo e i problemi di sicurezza relativi alle chiavi di crittografia statiche.

Con 802.1X, le credenziali utilizzate per l'autenticazione, come le password di accesso, non vengono mai trasmesse in chiaro o senza crittografia sul supporto wireless. Mentre i tipi di autenticazione 802.1X forniscono un'autenticazione avanzata per le LAN wireless, TKIP o AES sono necessari per la crittografia oltre a 802.1X poiché la crittografia WEP 802.11 standard è vulnerabile agli attacchi di rete.

Esistono diversi tipi di autenticazione 802.1X, ognuno dei quali fornisce un diverso approccio all'autenticazione, basandosi sullo stesso framework ed EAP per la comunicazione tra un client e un punto di accesso. I prodotti Cisco Aironet supportano più tipi di autenticazione 802.1X EAP di qualsiasi altro prodotto WLAN. I tipi supportati includono:

- [Cisco LEAP](#)
- [Autenticazione flessibile EAP tramite tunneling protetto \(EAP-FAST\)](#)
- EAP-Transport Layer Security (EAP-TLS)
- [Protocollo PEAP \(Protected Extensible Authentication Protocol\)](#)
- EAP-TLS (EAP-TTLS)
- EAP-SIM (EAP-Subscriber Identity Module)

Un altro vantaggio dell'autenticazione 802.1X è la gestione centralizzata per i gruppi di utenti WLAN, che include la rotazione delle chiavi basata su policy, l'assegnazione dinamica delle chiavi, l'assegnazione dinamica delle VLAN e la restrizione dell'SSID. Queste funzionalità consentono di ruotare le chiavi di crittografia.

Nella modalità operativa Personale, per l'autenticazione viene utilizzata una chiave (password) già condivisa. La modalità personale richiede solo un punto di accesso e un dispositivo client, mentre la modalità Enterprise richiede in genere un server RADIUS o un altro server di autenticazione sulla rete.

Questo documento offre esempi per configurare WPA2 (modalità Enterprise) e WPA2-PSK (modalità Personal) in una rete Cisco Unified Wireless.

## [Installazione della rete](#)

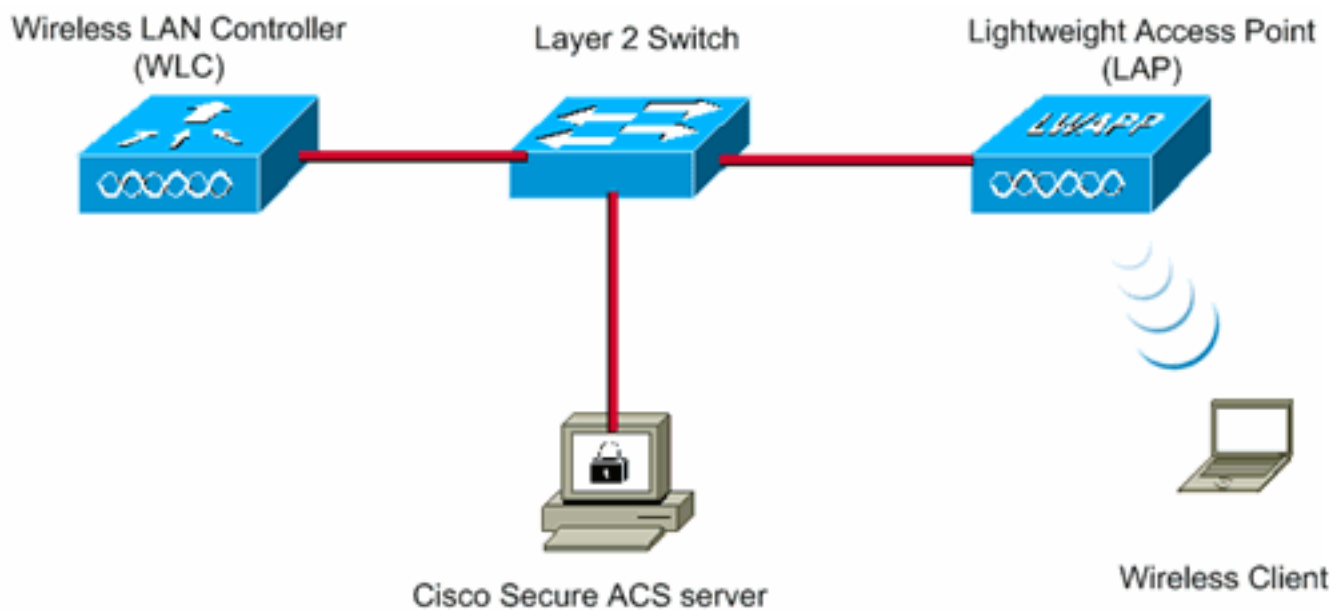
In questa configurazione, vengono collegati un Cisco 4404 WLC e un Cisco serie 1000 LAP tramite uno switch di layer 2. Allo stesso switch è collegato anche un server RADIUS esterno (Cisco Secure ACS). Tutti i dispositivi si trovano nella stessa subnet. Il punto di accesso (LAP) viene inizialmente registrato sul controller. È necessario creare due LAN wireless, una per la

modalità WPA2 Enterprise e l'altra per la modalità WPA2 Personal.

La modalità WPA2-Enterprise della WLAN (SSID: WPA2-Enterprise) utilizzerà EAP-FAST per autenticare i client wireless e AES per la crittografia. Il server Cisco Secure ACS verrà utilizzato come server RADIUS esterno per l'autenticazione dei client wireless.

La modalità WPA2-Personale WLAN (SSID: WPA2-PSK) utilizzerà la modalità WPA2-PSK per l'autenticazione con la chiave precondivisa "abcdefghijkl".

È necessario configurare i dispositivi per questa installazione:



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

## [Configurare i dispositivi per la modalità WPA2 Enterprise](#)

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Per configurare i dispositivi per la modalità operativa WPA2 Enterprise, eseguire la procedura seguente:

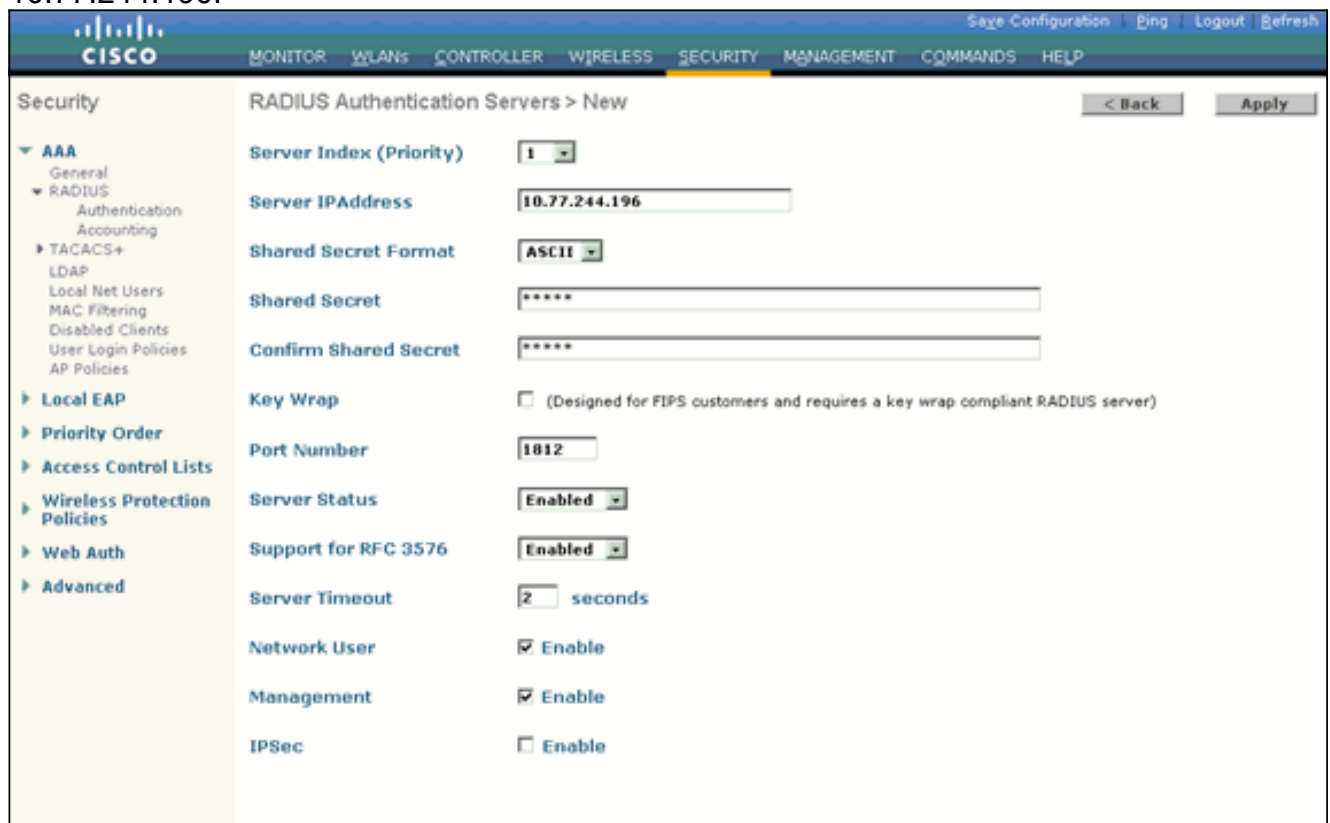
1. [Configurazione del WLC per l'autenticazione RADIUS tramite un server RADIUS esterno](#)
2. [Configurazione della WLAN per l'autenticazione in modalità enterprise WPA2 \(EAP-FAST\)](#)
3. [Configurare il client wireless per la modalità WPA2 Enterprise](#)

### [Configurazione del WLC per l'autenticazione RADIUS tramite un server RADIUS esterno](#)

Per inoltrare le credenziali dell'utente a un server RADIUS esterno, è necessario configurare il WLC. Il server RADIUS esterno convalida quindi le credenziali utente utilizzando EAP-FAST e fornisce l'accesso ai client wireless.

Per configurare il WLC per un server RADIUS esterno, completare la procedura seguente:

1. Scegliere **Sicurezza e Autenticazione RADIUS** dall'interfaccia utente del controller per visualizzare la pagina Server di autenticazione RADIUS. Quindi, fare clic su **New** (Nuovo) per definire un server RADIUS.
2. Definire i parametri del server RADIUS nella pagina **Server di autenticazione RADIUS > Nuovo**. Questi parametri includono: Indirizzo IP server RADIUS, Segreto condiviso, Numero porta server. In questo documento viene usato il server ACS con indirizzo IP 10.77.244.196.



The screenshot shows the Cisco WLC configuration interface for RADIUS Authentication Servers. The page title is "RADIUS Authentication Servers > New". The left sidebar shows the navigation menu with "Security" expanded and "RADIUS" selected. The main content area contains the following configuration fields:

Parameter	Value
Server Index (Priority)	1
Server IP Address	10.77.244.196
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

3. Fare clic su **Apply** (Applica).

## [Configurazione della WLAN per la modalità operativa WPA2 Enterprise](#)

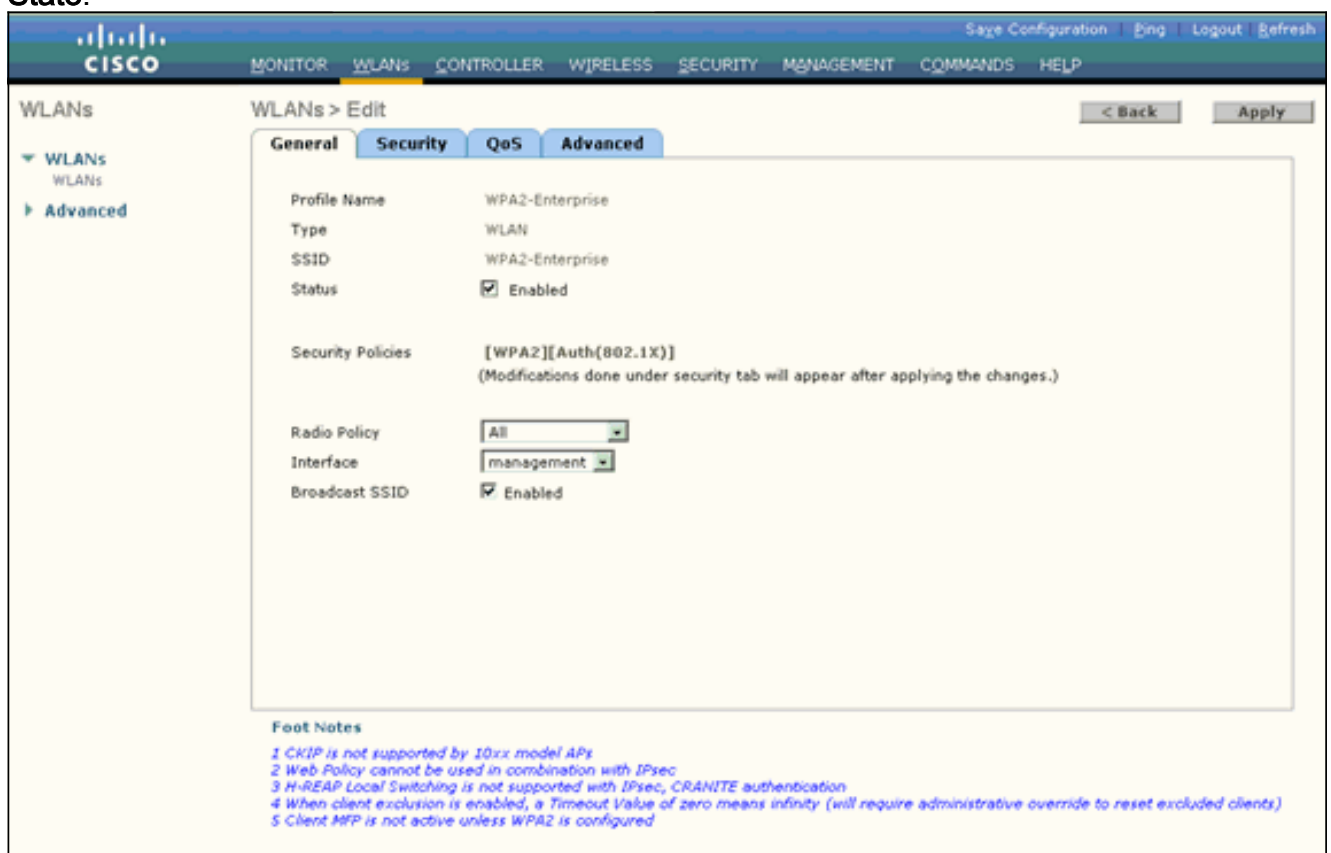
Quindi, configurare la WLAN che i client utilizzeranno per connettersi alla rete wireless. L'SSID WLAN per la modalità WPA2 enterprise sarà WPA2-Enterprise. In questo esempio la WLAN viene assegnata all'interfaccia di gestione.

Per configurare la WLAN e i parametri correlati, completare la procedura seguente:

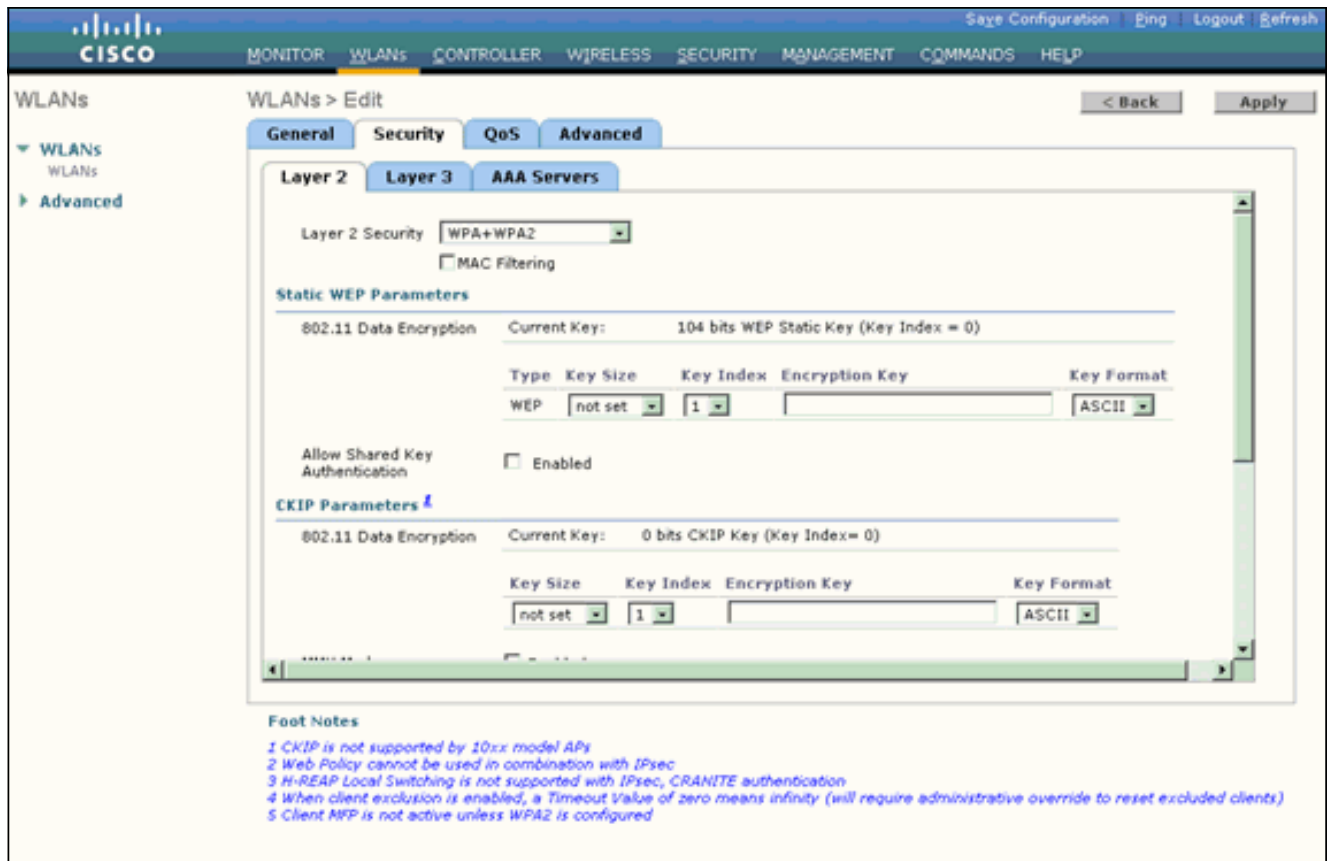
1. Fare clic su **WLAN** dall'interfaccia utente del controller per visualizzare la pagina WLAN. In questa pagina vengono elencate le WLAN esistenti sul controller.
2. Per creare una nuova WLAN, fare clic su **New** (Nuovo).
3. Immettere il nome dell'SSID della WLAN e il nome del profilo nella pagina **WLAN > Nuovo**. Quindi fare clic su **Apply** (Applica). In questo esempio viene utilizzato **WPA2-Enterprise** come SSID.



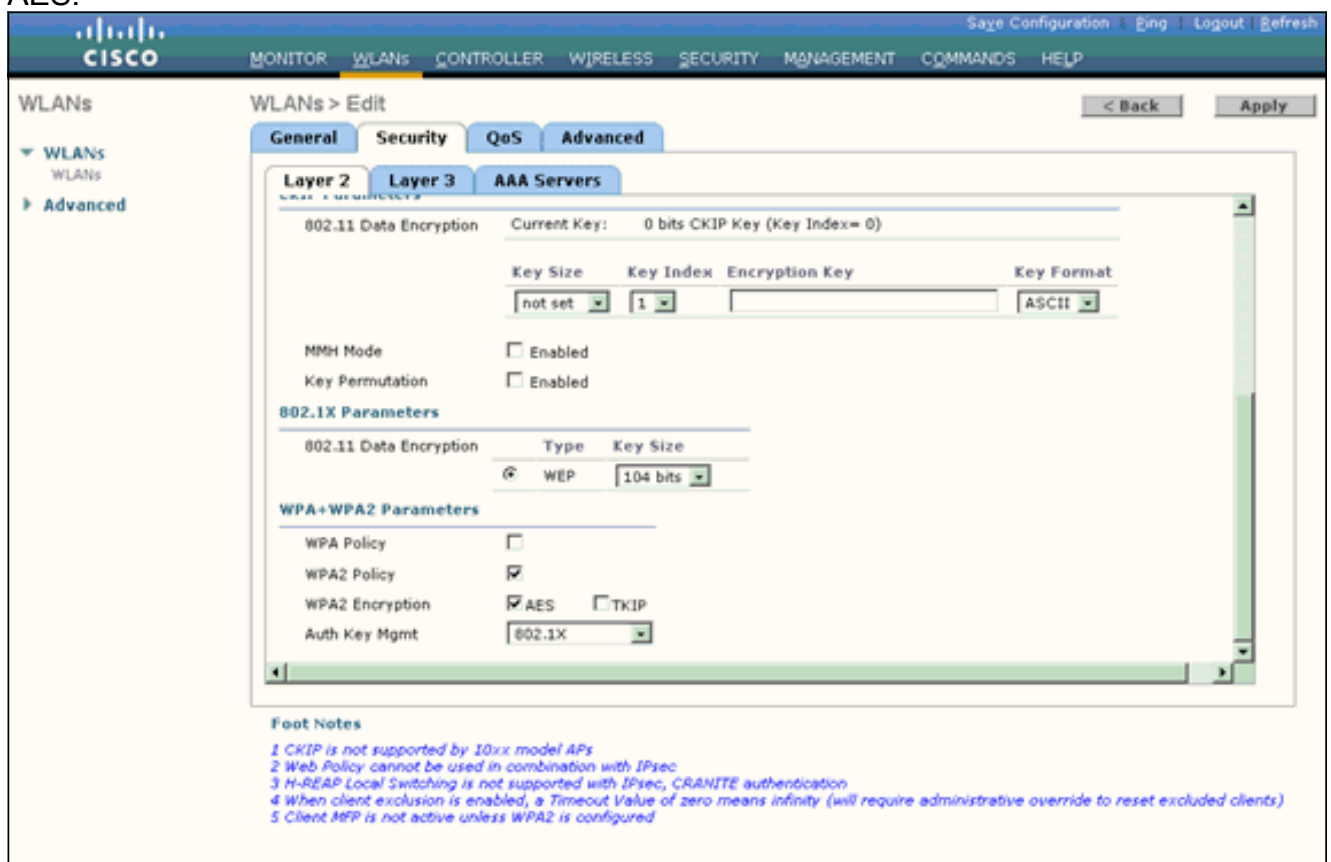
4. Dopo aver creato una nuova WLAN, viene visualizzata la pagina **WLAN > Modifica** per la nuova WLAN. In questa pagina è possibile definire vari parametri specifici per la WLAN. Sono inclusi i criteri generali, i criteri di sicurezza, i criteri QoS e i parametri avanzati.
5. Per abilitare la WLAN, in Criteri generali selezionare la casella di controllo **Stato**.



6. Se si desidera che l'access point trasmetta il SSID nei frame del beacon, selezionare la casella di controllo **Broadcast SSID**.
7. Fare clic sulla scheda **Protezione**. In Protezione di livello 2, scegliere **WPA+WPA2**. In questo modo viene abilitata l'autenticazione WPA per la WLAN.



8. Scorrere la pagina verso il basso per modificare i **parametri WPA+WPA2**. Nell'esempio vengono selezionati i criteri WPA2 e la crittografia AES.



9. In Gestione chiavi di autenticazione scegliere **802.1x**. Ciò consente a WPA2 di utilizzare l'autenticazione 802.1x/EAP e la crittografia AES per la WLAN.
10. Fare clic sulla scheda **Server AAA**. In Server di autenticazione scegliere l'indirizzo IP del server appropriato. Nell'esempio, 10.77.244.196 viene usato come server

## RADIUS.

The screenshot shows the Cisco WLAN configuration interface. The main menu includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The current view is 'WLANs > Edit' with tabs for General, Security, QoS, and Advanced. Under the Advanced tab, there are sub-tabs for Layer 2, Layer 3, and AAA Servers. The AAA Servers section is active, showing a form to configure AAA servers. The form includes a section for 'Radius Servers' with columns for 'Authentication Servers' and 'Accounting Servers'. There are three rows for 'Server 1', 'Server 2', and 'Server 3'. The 'Accounting Servers' section has an 'Enabled' checkbox. The 'Local EAP Authentication' section has an 'Enabled' checkbox. The 'Foot Notes' section contains five notes: 1 CRIP is not supported by 10xx model APs, 2 Web Policy cannot be used in combination with IPsec, 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication, 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients), 5 Client MFP is not active unless WPA2 is configured.

11. Fare clic su **Apply** (Applica). **Nota:** questa è l'unica impostazione EAP da configurare sul controller per l'autenticazione EAP. Tutte le altre configurazioni specifiche di EAP-FAST devono essere eseguite sul server RADIUS e sui client che devono essere autenticati.

## [Configurare il server RADIUS per l'autenticazione in modalità Enterprise WPA2 \(EAP-FAST\)](#)

Nell'esempio, Cisco Secure ACS viene usato come server RADIUS esterno. Per configurare il server RADIUS per l'autenticazione EAP-FAST, attenersi alla procedura seguente:

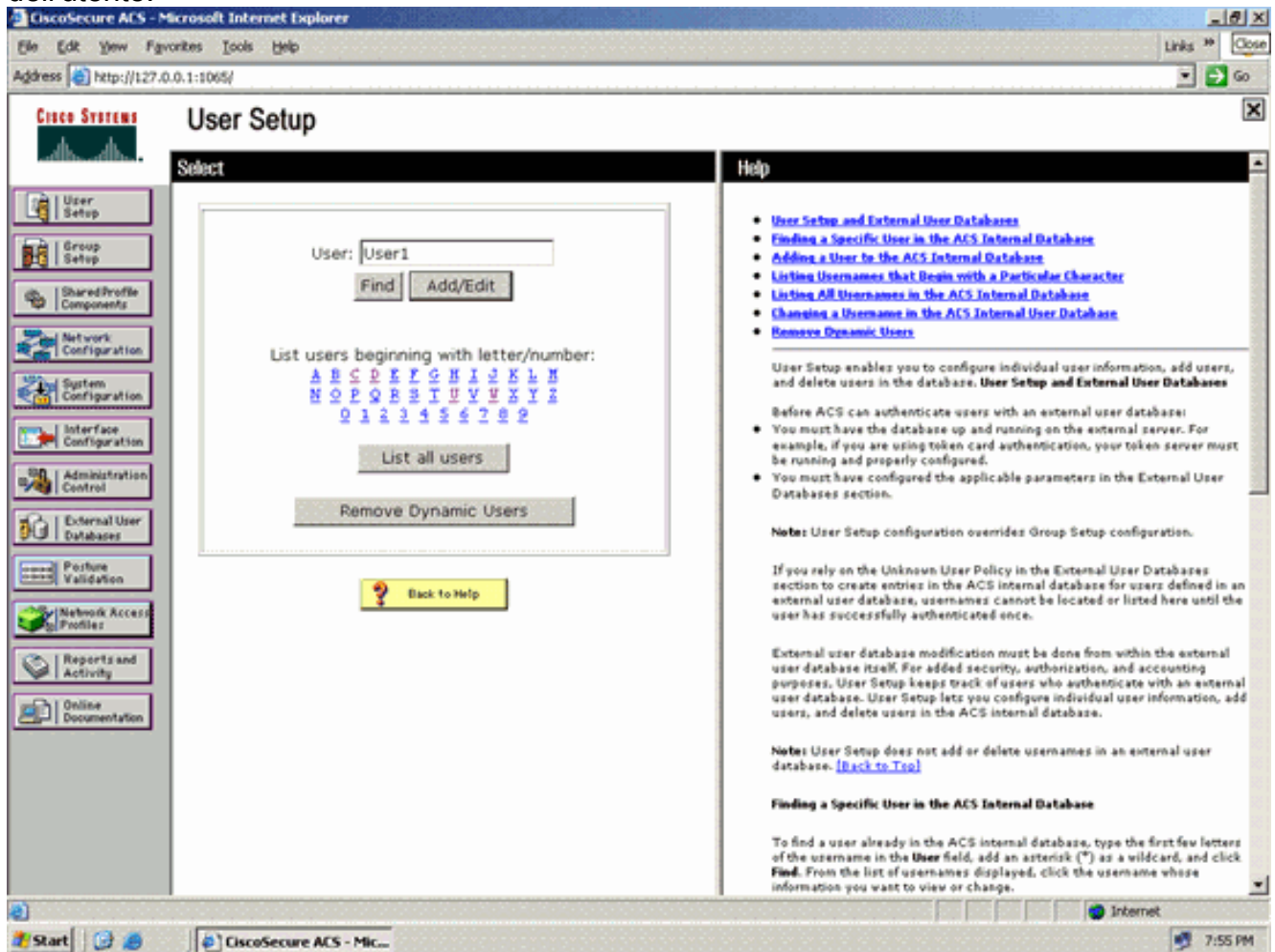
1. [Crea un database utenti per autenticare i client](#)
2. [Aggiungere il WLC come client AAA al server RADIUS](#)
3. [Configurazione dell'autenticazione EAP-FAST sul server RADIUS con provisioning PAC in banda anonimo](#) **Nota:** EAP-FAST può essere configurato con la funzione di preparazione anonima della PAC in banda o con la funzione di preparazione autenticata della PAC in banda. In questo esempio viene utilizzata la preparazione anonima della PAC in banda. Per informazioni dettagliate ed esempi sulla configurazione di EAP FAST con il provisioning PAC in banda anonimo e il provisioning in banda autenticato, fare riferimento agli [esempi di autenticazione EAP-FAST con i controller LAN wireless e di configurazione del server RADIUS esterno](#).

## [Creazione di un database utenti per autenticare i client EAP-FAST](#)

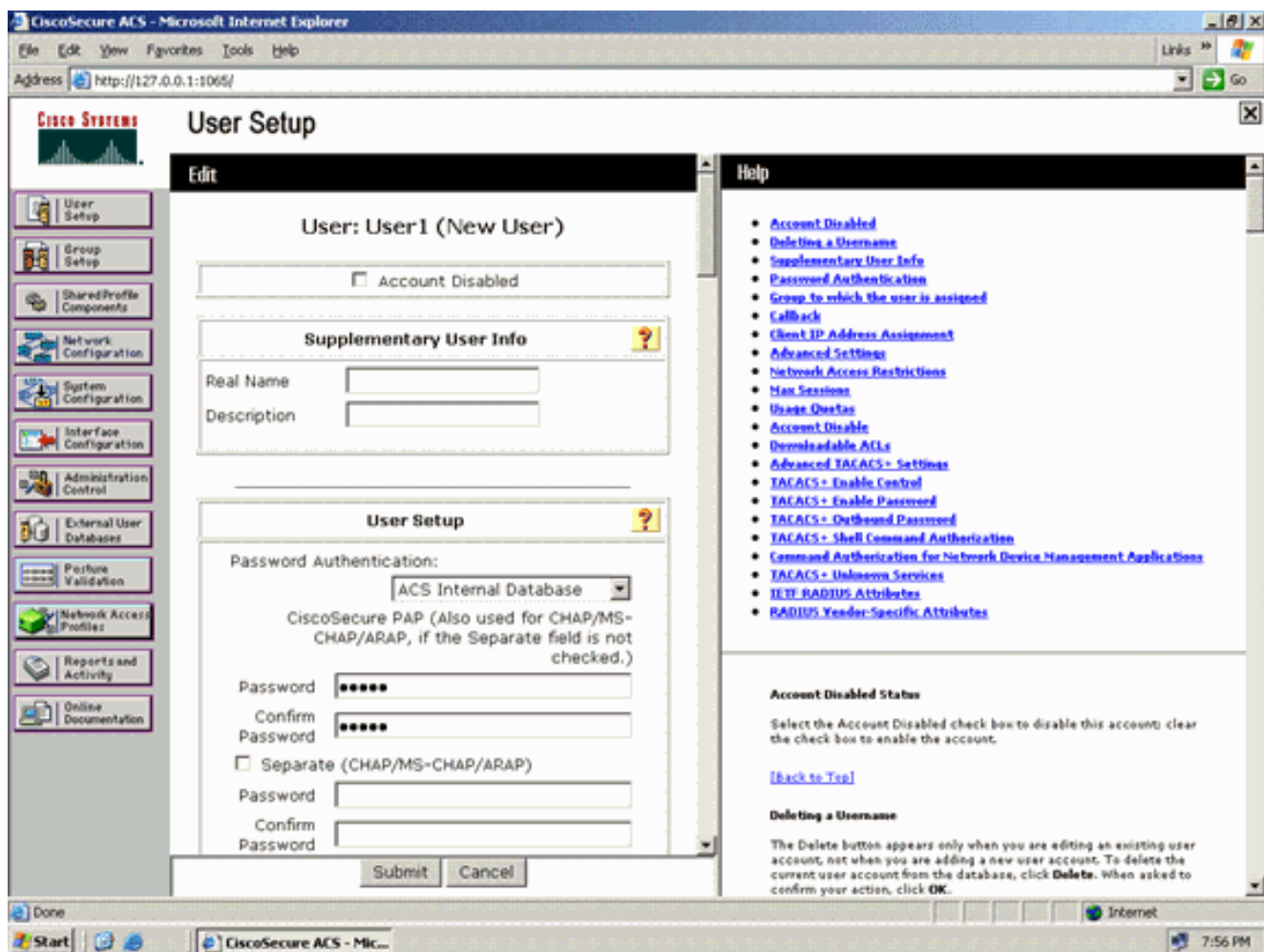
Completare questi passaggi per creare un database utenti per i client EAP-FAST sul server ACS. In questo esempio vengono configurati il nome utente e la password del client EAP-FAST rispettivamente come User1 e User1.



1. Dalla GUI di ACS nella barra di navigazione, selezionare **User Setup** (Configurazione utente). Creare un nuovo utente senza fili e quindi fare clic su **Aggiungi/Modifica** per accedere alla pagina Modifica dell'utente.



2. Nella pagina Modifica della procedura guidata, configurare il nome reale e la descrizione, nonché le impostazioni della password, come illustrato in questo esempio. In questo documento viene usato il **database interno ACS** per l'autenticazione tramite password.

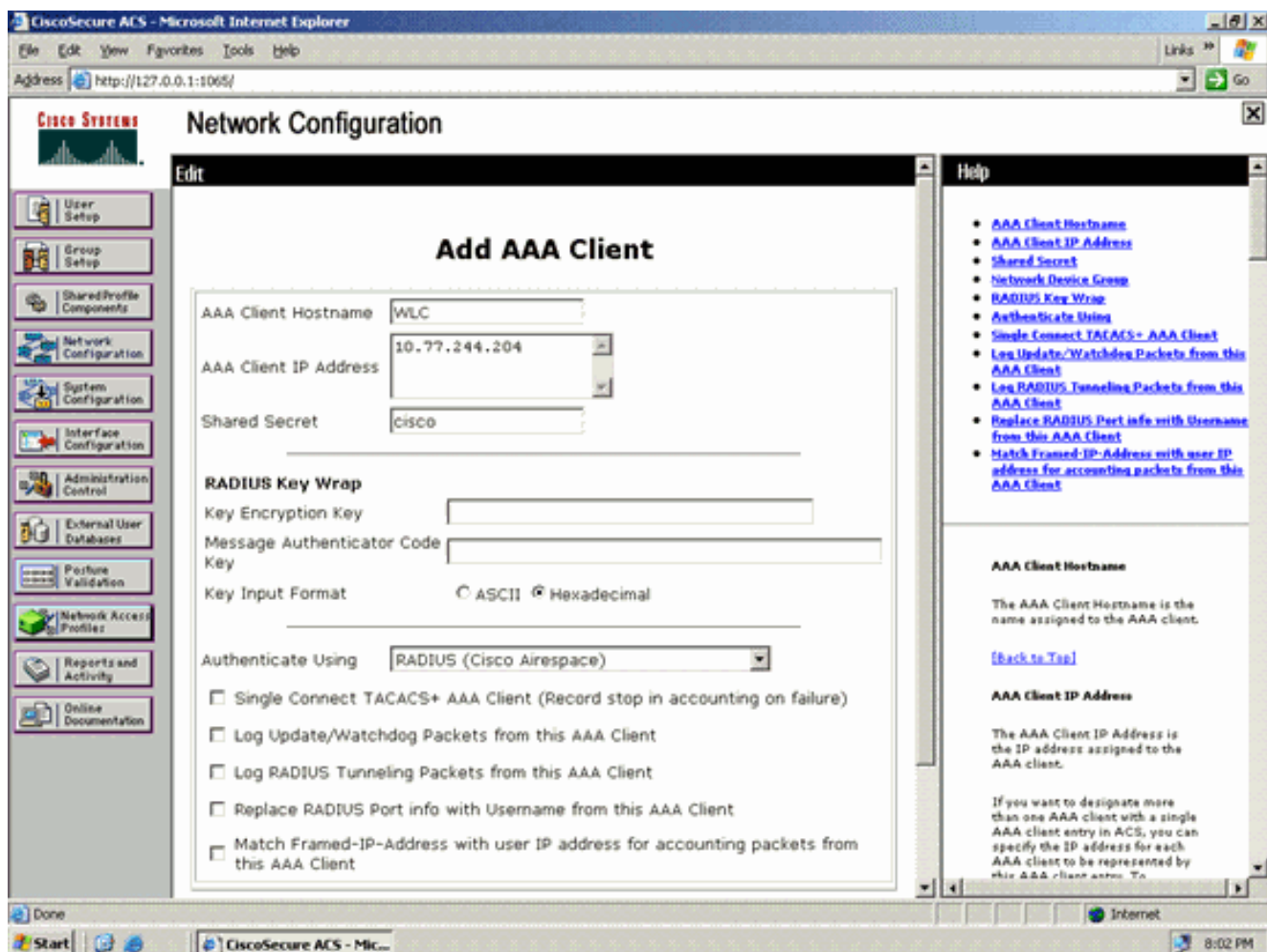


3. Selezionare **ACS Internal Database** (Database interno ACS) dalla casella a discesa Password Authentication (Autenticazione password).
4. Configurare tutti gli altri parametri obbligatori e fate clic su **Invia (Submit)**.

### [Aggiungere il WLC come client AAA al server RADIUS](#)

Completare questa procedura per definire il controller come client AAA sul server ACS:

1. Fare clic su **Network Configuration** (Configurazione di rete) dall'interfaccia utente di ACS. Nella sezione Add AAA client della pagina Network Configuration, fare clic su **Add Entry** per aggiungere il WLC come client AAA al server RADIUS.
2. Dalla pagina Client AAA, definire il nome del WLC, l'indirizzo IP, il segreto condiviso e il metodo di autenticazione (RADIUS/Cisco Airespace). Per altri server di autenticazione non ACS, consultare la documentazione del produttore.



**Nota:** la chiave segreta condivisa configurata sul WLC e sul server ACS deve corrispondere. Il segreto condiviso fa distinzione tra maiuscole e minuscole.

3. Fare clic su **Invia+Applica**.

## [Configurazione dell'autenticazione EAP-FAST sul server RADIUS con provisioning PAC in banda anonimo](#)

### Provisioning in banda anonimo

Questo è uno dei due metodi di provisioning in banda con cui l'ACS stabilisce una connessione protetta con il client dell'utente finale allo scopo di fornire al client una nuova PAC. Questa opzione consente un handshake TLS anonimo tra il client utente finale e ACS.

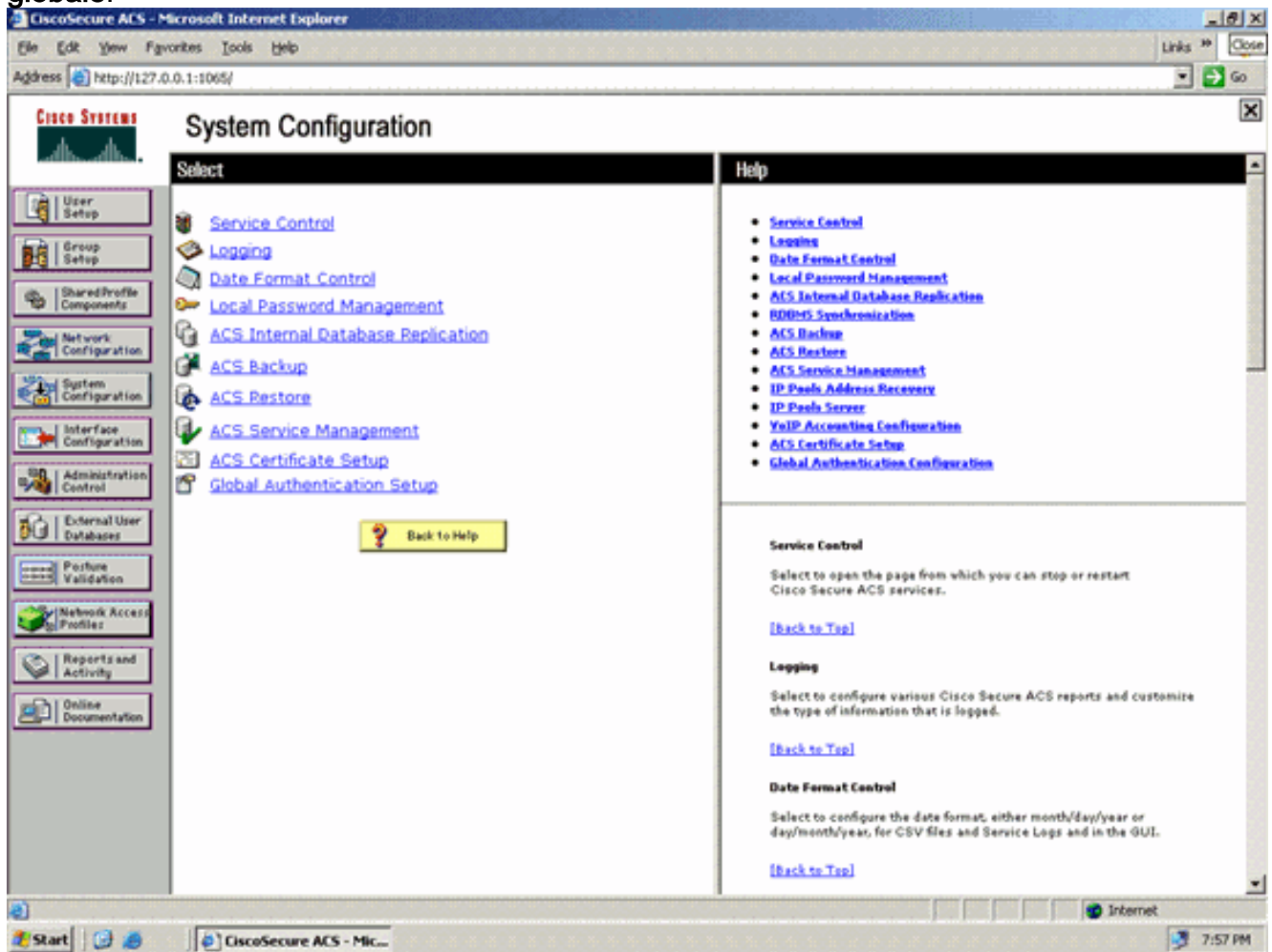
Questo metodo funziona all'interno di un tunnel ADHP (Authenticated Diffie-Hellman Key Agreement Protocol) prima che il peer autentichi il server ACS.

Quindi, ACS richiede l'autenticazione EAP-MS-CHAPv2 dell'utente. Una volta completata l'autenticazione dell'utente, ACS stabilisce un tunnel Diffie-Hellman con il client dell'utente finale. L'ACS genera una PAC per l'utente e la invia al client dell'utente finale in questo tunnel, insieme alle informazioni sull'ACS. Questo metodo di provisioning utilizza EAP-MSCHAPv2 come metodo di autenticazione nella fase zero e EAP-GTC nella fase due.

Poiché è stato eseguito il provisioning di un server non autenticato, non è possibile utilizzare una password in testo normale. Pertanto, è possibile utilizzare solo le credenziali MS-CHAP all'interno del tunnel. MS-CHAPv2 viene utilizzato per provare l'identità del peer e ricevere una PAC per ulteriori sessioni di autenticazione (EAP-MS-CHAP verrà utilizzato solo come metodo interno).

Completare questa procedura per configurare l'autenticazione EAP-FAST nel server RADIUS per il provisioning in banda anonimo:

1. Fare clic su **Configurazione di sistema** dall'interfaccia utente del server RADIUS. Dalla pagina Configurazione di sistema, scegliere **Configurazione autenticazione globale**.



2. Dalla pagina di impostazione dell'autenticazione globale, fare clic su **Configurazione EAP-FAST** per accedere alla pagina di impostazione di EAP-FAST.

CiscoSecure ACS - Microsoft Internet Explorer

Address: http://127.0.0.1:1005/

## System Configuration

### EAP Configuration

**PEAP**

- Allow EAP-MSCHAPv2
- Allow EAP-GTC
- Allow Posture Validation

---

Allow EAP-TLS

Select one or more of the following options:

- Certificate SAN comparison
- Certificate CN comparison
- Certificate Binary comparison

EAP-TLS session timeout (minutes):

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

**EAP-FAST**

[EAP-FAST Configuration](#)

**EAP-TLS**

- Allow EAP-TLS

Select one or more of the following options:

- Certificate SAN comparison

Submit Submit + Restart Cancel

### Help

Use this page to specify settings for various authentication protocols.

- [EAP Configuration](#)
- [PEAP](#)
- [EAP-FAST](#)
- [EAP-TLS](#)
- [LEAP](#)
- [EAP-MD5](#)
- [AP EAP Request Timeout](#)
- [MS-CHAP Configuration](#)

**EAP Configuration**

EAP is a flexible request/response protocol for arbitrary authentication information (RFC 2284). EAP is layered on top of another protocol such as UDP, 802.1x or RADIUS and supports multiple "authentication" types.

[\[Back to Top\]](#)

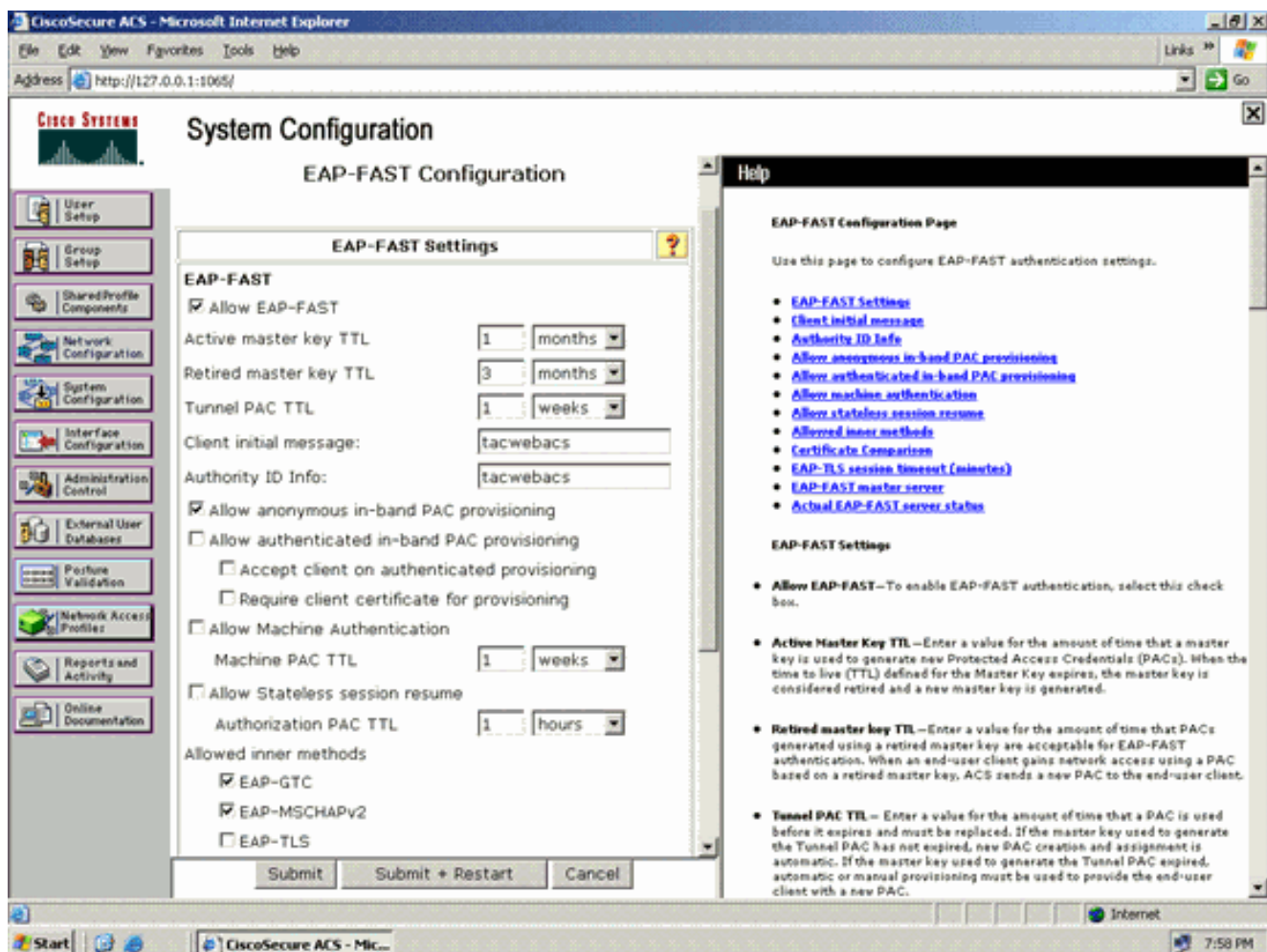
**PEAP**

PEAP is the outer layer protocol for the secure tunnel.

*Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have completed the required steps on the ACS Certificate Setup page.*

- Allow EAP-MSCHAPv2** – Use to enable EAP-MSCHAPv2 within MS PEAP authentication. Enable this protocol for any repository that supports MS-CHAPv2, such as Microsoft AD, and the ACS Internal Database.

3. Nella pagina Impostazioni EAP-FAST selezionare la casella di controllo **Consenti EAP-FAST** per abilitare EAP-FAST nel server RADIUS.



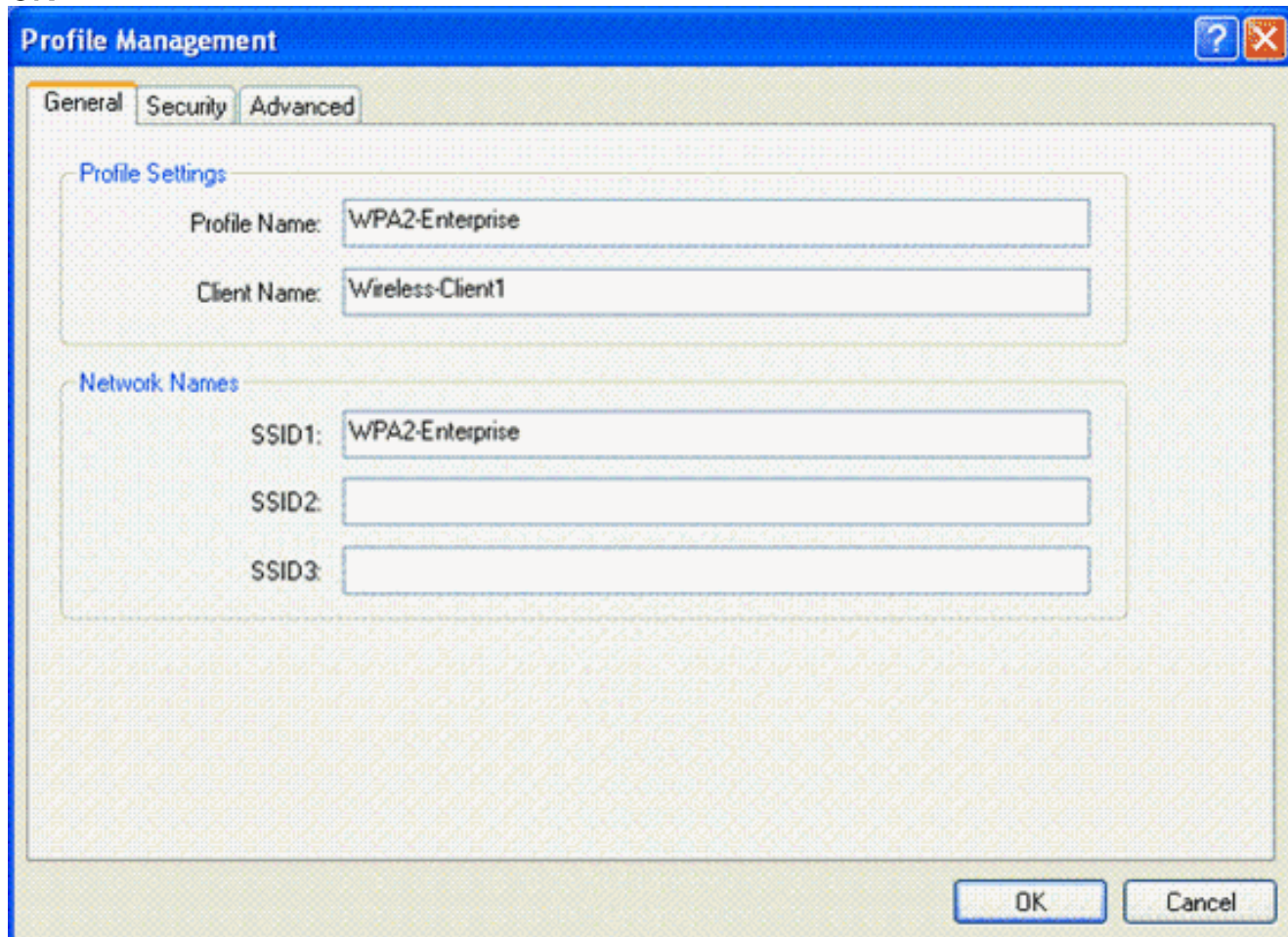
4. Configurare i valori TTL (Time-to-Live) della chiave master attiva/ritirata in base alle esigenze oppure impostarli sul valore predefinito, come illustrato in questo esempio. Per informazioni sulle chiavi master attive e ritirate, fare riferimento a Chiavi master. Inoltre, fare riferimento a Chiavi master e TTL PAC per ulteriori informazioni. Il campo Authority ID Info (Informazioni ID autorità) rappresenta l'identità testuale del server ACS, che un utente finale può utilizzare per determinare il server ACS da autenticare. Compilare questo campo è obbligatorio. Il campo Messaggio iniziale di visualizzazione client specifica il messaggio da inviare agli utenti che eseguono l'autenticazione con un client EAP-FAST. La lunghezza massima è di 40 caratteri. Il messaggio iniziale verrà visualizzato solo se il client dell'utente finale supporta la visualizzazione.
5. Se si desidera che ACS esegua la preparazione anonima della PAC in banda, selezionare la casella di controllo **Consenti preparazione anonima della PAC in banda**.
6. **Metodi interni consentiti** - Questa opzione determina quali metodi EAP interni possono essere eseguiti all'interno del tunnel EAP-FAST TLS. Per il provisioning in banda anonimo, è necessario abilitare EAP-GTC e EAP-MS-CHAP per la compatibilità con le versioni precedenti. Se si seleziona Consenti preparazione PAC in banda anonima, è necessario selezionare EAP-MS-CHAP (fase zero) e EAP-GTC (fase due).

## [Configurazione del client wireless per la modalità di funzionamento WPA2 Enterprise](#)

Il passaggio successivo consiste nel configurare il client wireless per la modalità operativa WPA2 Enterprise.

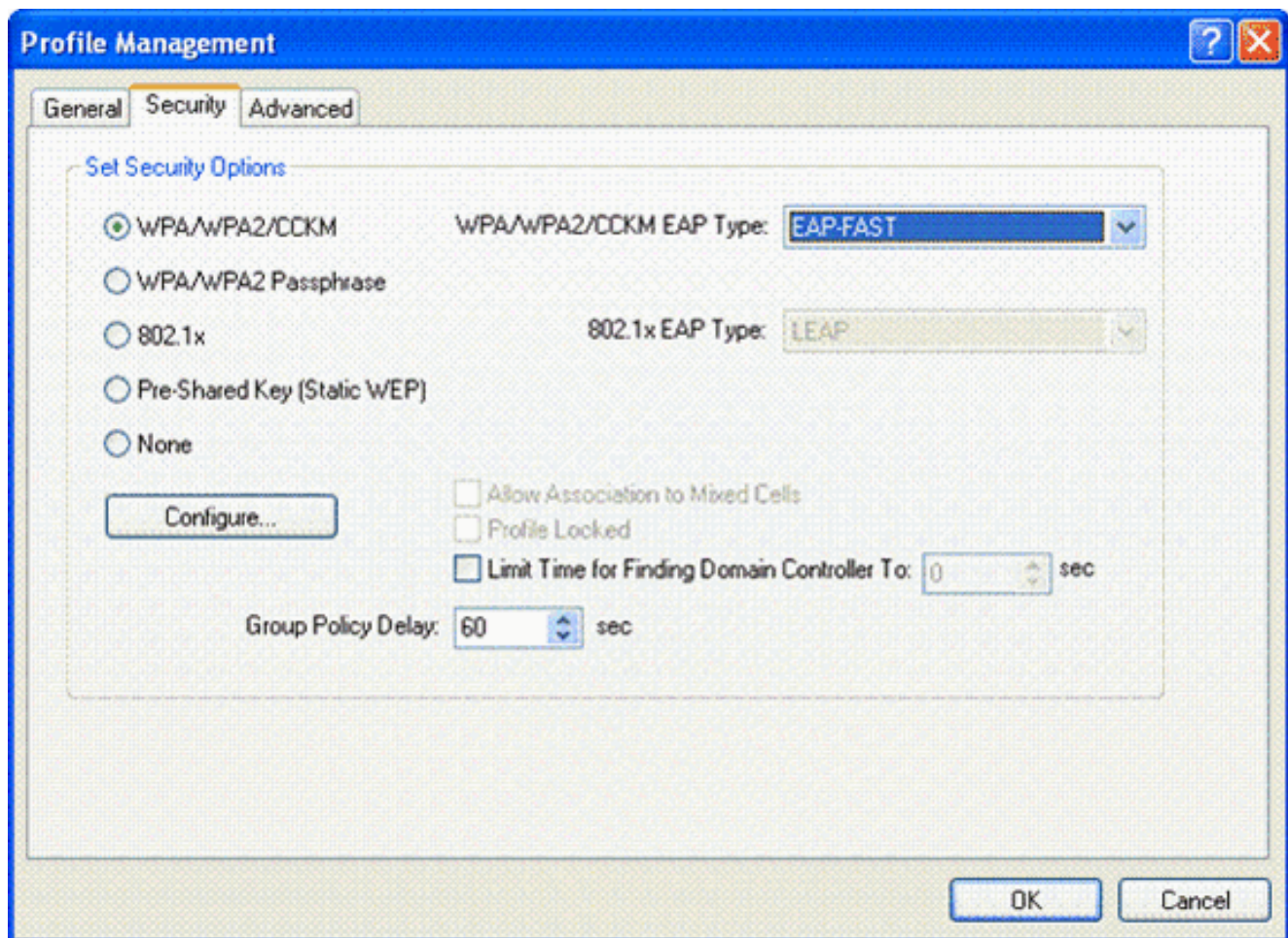
Completare questa procedura per configurare il client wireless per la modalità WPA2 Enterprise.

1. Dalla finestra Aironet Desktop Utility, fare clic su **Profile Management > New** (Gestione profili > Nuovo) per creare un profilo per l'utente WPA2-Enterprise WLAN. Come accennato in precedenza, in questo documento il nome WLAN/SSID viene usato come **WPA2-Enterprise** per il client wireless.
2. Dalla finestra Gestione profili, fare clic sulla scheda **Generale** e configurare il Nome profilo, il Nome client e il Nome SSID come mostrato in questo esempio. Quindi, fare clic su **OK**



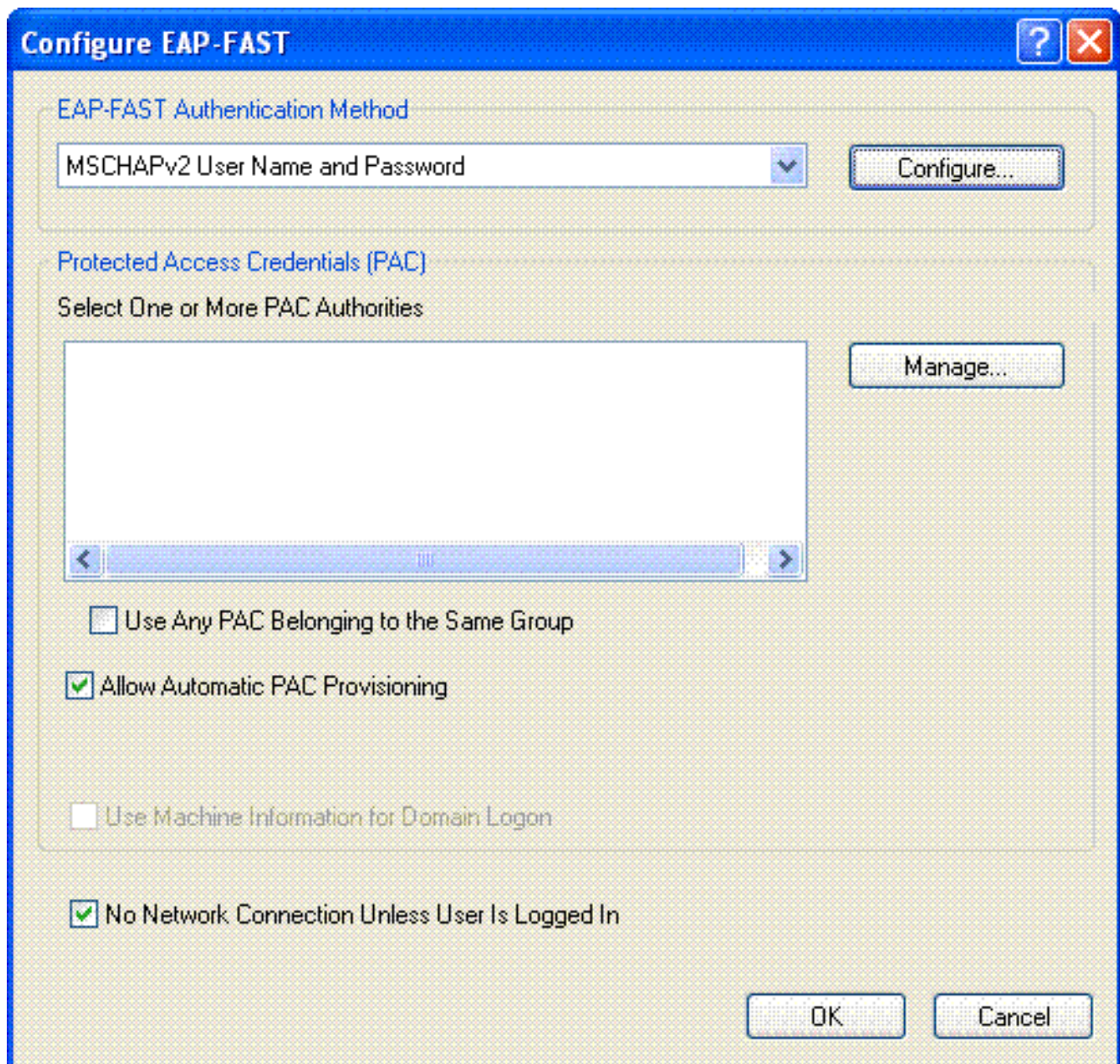
The screenshot shows the 'Profile Management' dialog box with the 'General' tab active. The 'Profile Settings' section contains two text boxes: 'Profile Name' with the value 'WPA2-Enterprise' and 'Client Name' with the value 'Wireless-Client1'. The 'Network Names' section contains three text boxes: 'SSID1' with the value 'WPA2-Enterprise', 'SSID2' which is empty, and 'SSID3' which is empty. At the bottom right, there are 'OK' and 'Cancel' buttons.

3. Fare clic sulla scheda **Security** (Sicurezza) e scegliere **WPA/WPA2/CCKM** per abilitare la modalità di funzionamento WPA2. In WPA/WPA2/CCKM EAP Type (Tipo EAP WPA/WPA2/CCKM), selezionare **EAP-FAST** (EAP-FAST). Per configurare l'impostazione EAP-FAST, fare clic su **Configure** (Configura).

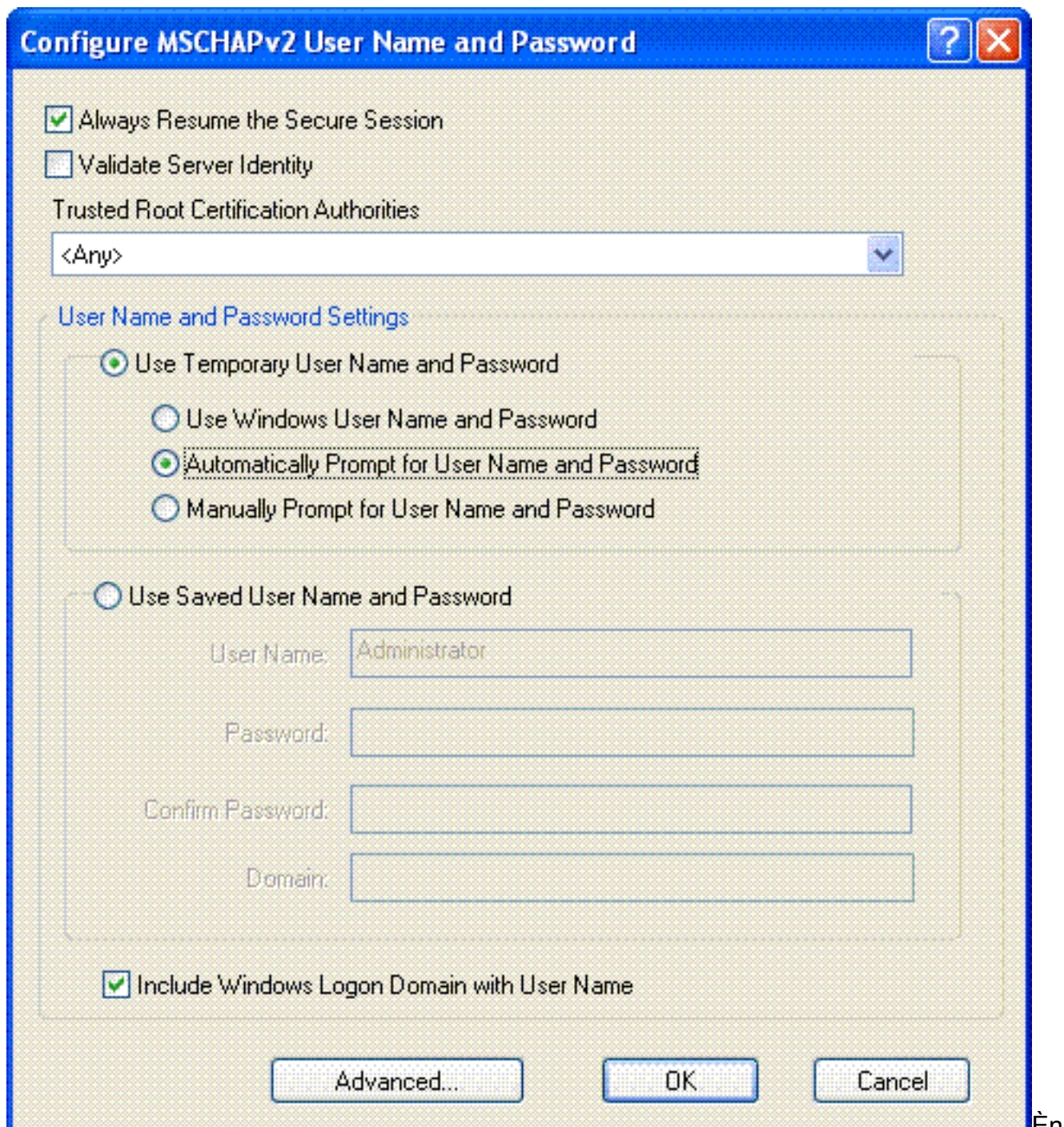


4. Nella finestra Configura EAP-FAST selezionare la casella di controllo **Consenti preparazione automatica PAC**. Se si desidera configurare la preparazione PAC anonima, EAP-MS-CHAP verrà utilizzato come unico metodo interno nella fase zero.





5. Scegliere Nome utente e password MSCHAPv2 come metodo di autenticazione nella casella a discesa Metodo di autenticazione EAP-FAST. Fare clic su **Configura**.
6. Nella finestra Configura nome utente e password MSCHAPv2 scegliere le impostazioni appropriate per il nome utente e la password. In questo esempio viene selezionata l'opzione **Richiedi automaticamente nome utente e password**.



È necessario registrare lo stesso nome utente e la stessa password presso l'ACS. Come accennato in precedenza, in questo esempio vengono utilizzati rispettivamente User1 e User1 come nome utente e password. Si noti inoltre che si tratta di un provisioning in banda anonimo. Il client non può pertanto convalidare il certificato del server. È necessario verificare che la casella di controllo Convalida identità server sia deselezionata.

7. Fare clic su **OK**.

### [Verifica modalità di funzionamento WPA2 Enterprise](#)

Per verificare il corretto funzionamento della configurazione in modalità WPA2 Enterprise, completare i seguenti passaggi:

1. Dalla finestra Aironet Desktop Utility, selezionare il profilo **WPA2-Enterprise** e fare clic su **Activate** (Attiva) per attivare il profilo client wireless.
2. Se è stato abilitato MS-CHAP ver2 come autenticazione, il client richiederà il nome utente e

**Enter Wireless Network Password**

Please enter your EAP-FAST username and password to log on to the wireless network.

User Name : User1

Password : ●●●●●●

Log on to :

Card Name : Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name : WPA-Enterprise

OK Cancel

la password.

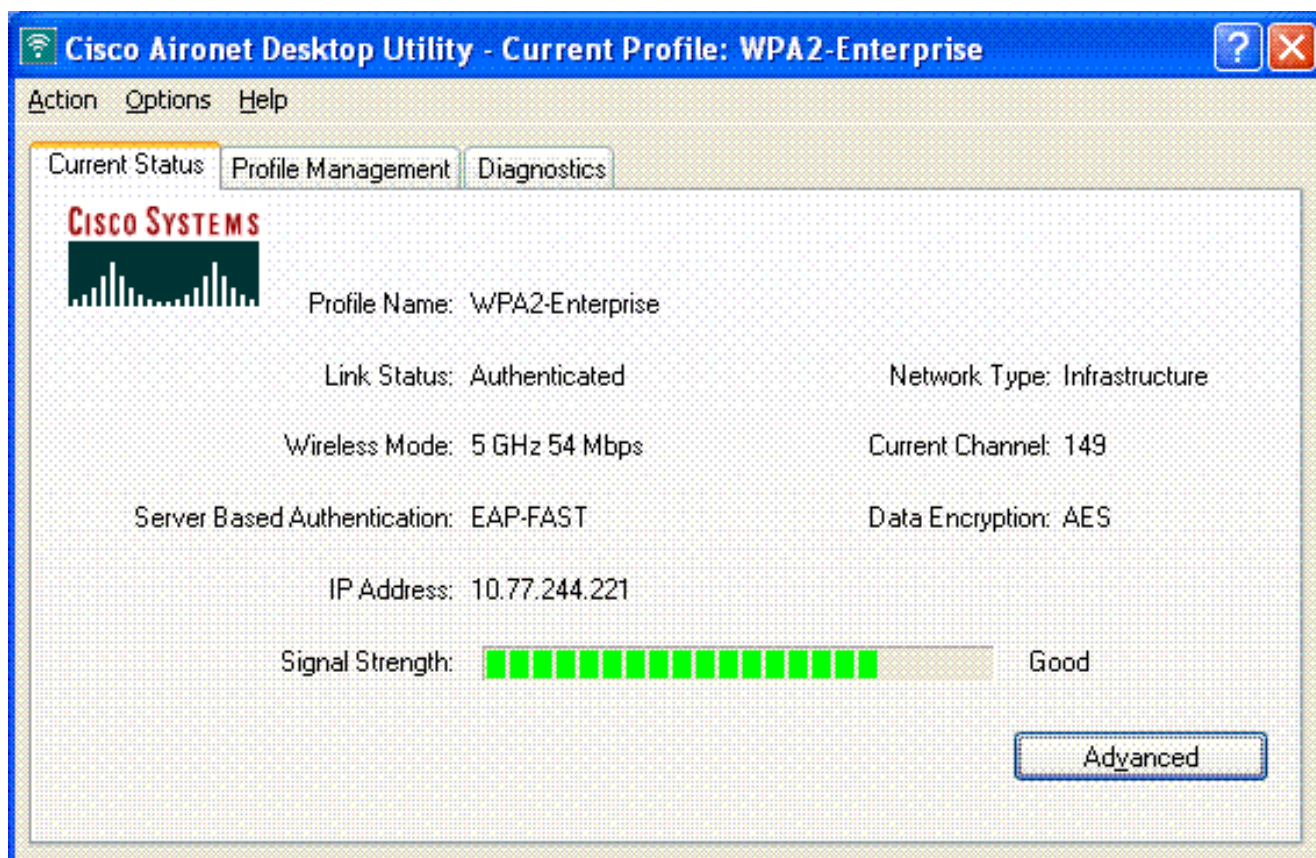
3. Durante l'elaborazione EAP-FAST dell'utente, il client richiederà la PAC al server RADIUS. Se si fa clic su **Sì**, viene avviata la preparazione della PAC.

**EAP-FAST Authentication**

You do not have a valid PAC from the authentication server. Do you want to proceed and request automatic provisioning?

Yes No

4. Una volta completata la preparazione della PAC nella fase zero, seguire la fase uno e due ed eseguire con successo la procedura di autenticazione. Una volta completata l'autenticazione, il client wireless viene associato alla WLAN WPA2-Enterprise. Ecco lo screenshot:



È inoltre possibile verificare se il server RADIUS riceve e convalida la richiesta di autenticazione dal client wireless. A tale scopo, controllare i report Autenticazioni superate e Tentativi non riusciti sul server ACS. Questi report sono disponibili in Report e attività sul server ACS.

## [Configurare i dispositivi per la modalità personale WPA2](#)

Per configurare i dispositivi per la modalità di funzionamento WPA2-Personale, attenersi alla seguente procedura:

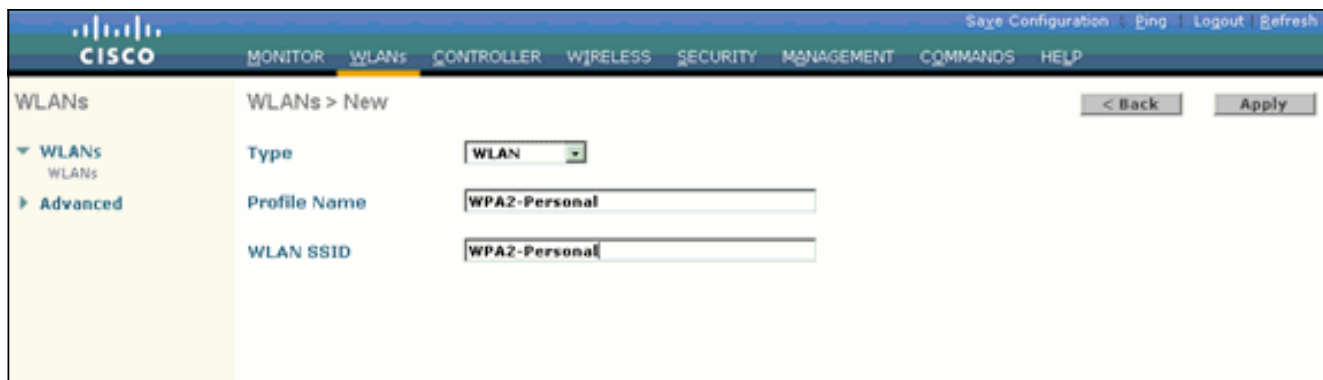
1. [Configurazione della WLAN per l'autenticazione in modalità personale WPA2](#)
2. [Configurare il client wireless per la modalità personale WPA2](#)

### [Configurazione della WLAN per la modalità di funzionamento personale di WPA2](#)

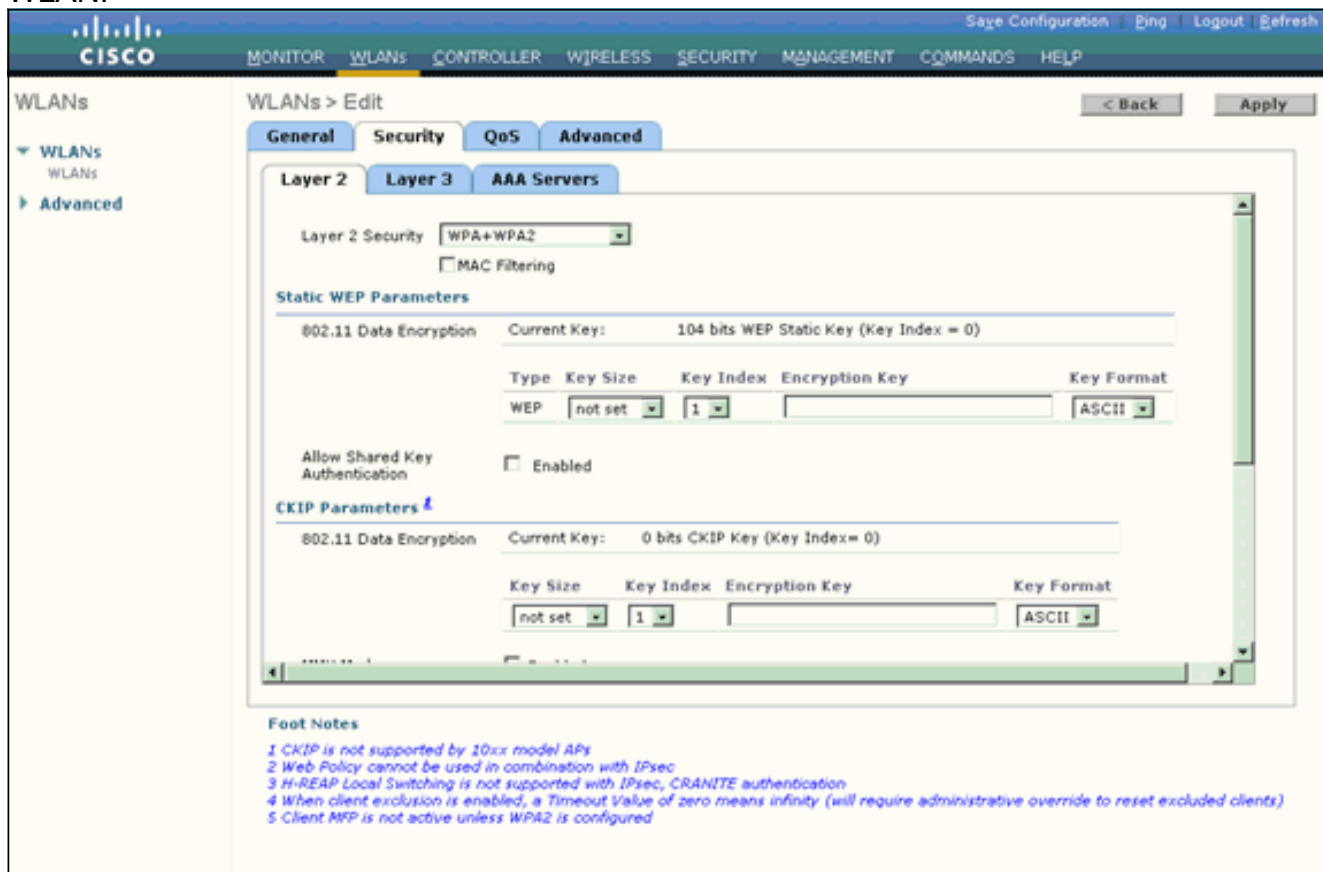
È necessario configurare la WLAN che i client utilizzeranno per connettersi alla rete wireless. L'SSID WLAN per la modalità personale WPA2 sarà WPA2-Personale. In questo esempio la WLAN viene assegnata all'interfaccia di gestione.

Per configurare la WLAN e i parametri correlati, completare la procedura seguente:

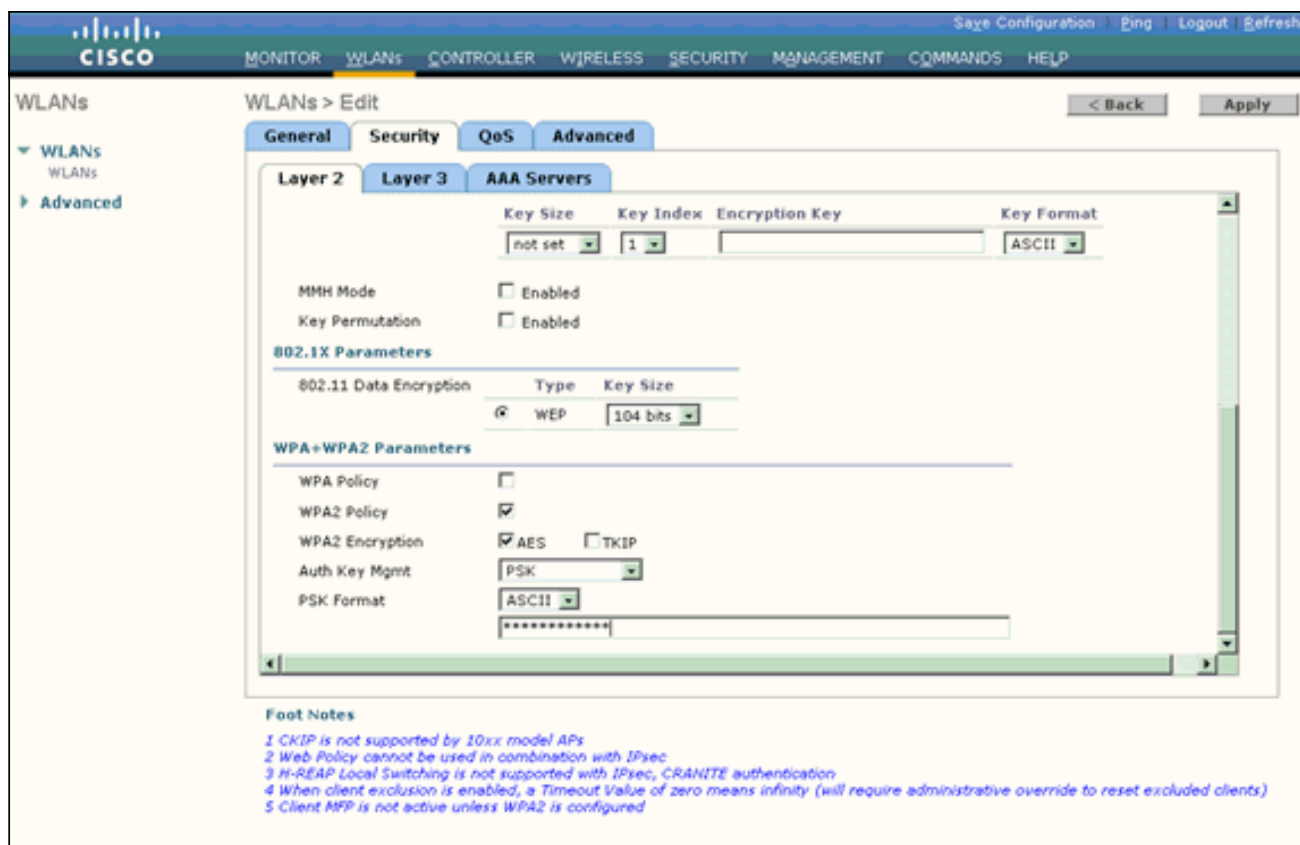
1. Fare clic su **WLAN** dall'interfaccia utente del controller per visualizzare la pagina WLAN. In questa pagina vengono elencate le WLAN esistenti sul controller.
2. Per creare una nuova WLAN, fare clic su **New** (Nuovo).
3. Immettere il nome dell'SSID della WLAN, il nome del profilo e l'ID della WLAN nella pagina WLAN > Nuovo. Quindi fare clic su **Apply** (Applica). In questo esempio viene utilizzato **WPA2-Personal** come SSID.



4. Dopo aver creato una nuova WLAN, viene visualizzata la pagina **WLAN > Modifica** per la nuova WLAN. In questa pagina è possibile definire vari parametri specifici per la WLAN. Sono inclusi i criteri generali, i criteri di sicurezza, i criteri QoS e i parametri avanzati.
5. Per abilitare la WLAN, in Criteri generali selezionare la casella di controllo **Stato**.
6. Se si desidera che l'access point trasmetta il SSID nei frame del beacon, selezionare la casella di controllo **Broadcast SSID**.
7. Fare clic sulla scheda **Protezione**. In Protezione livello, scegliere **WPA+WPA2**. In questo modo viene abilitata l'autenticazione WPA per la WLAN.



8. Scorrere la pagina verso il basso per modificare i **parametri WPA+WPA2**. Nell'esempio vengono selezionati i criteri WPA2 e la crittografia AES.
9. In Gestione chiavi di autenticazione scegliere **PSK** per abilitare WPA2-PSK.
10. Immettere la chiave già condivisa nel campo appropriato, come illustrato.



**Nota:** la chiave già condivisa utilizzata sul WLC deve corrispondere a quella configurata sui client wireless.

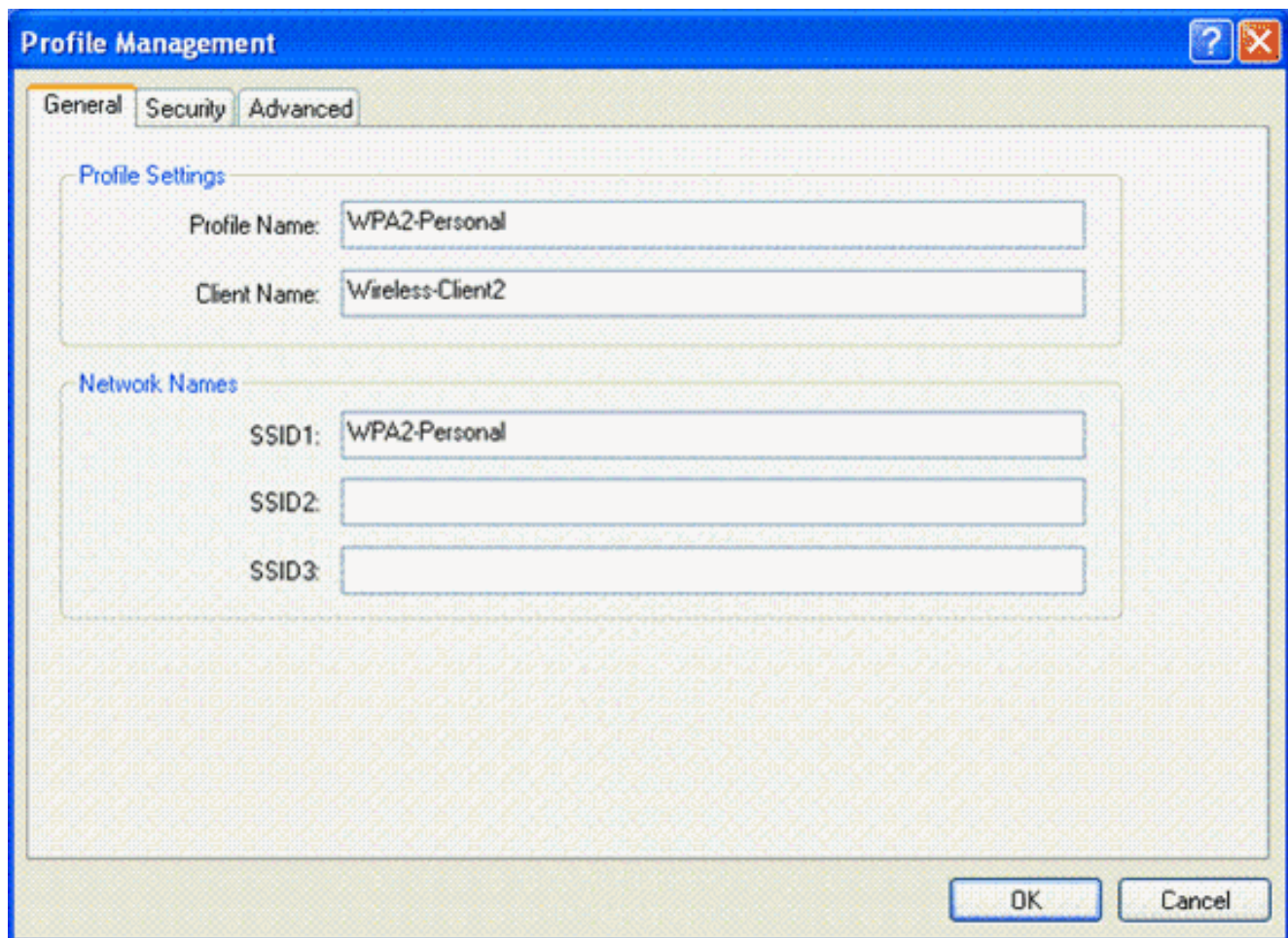
11. Fare clic su **Apply** (Applica).

## [Configurare il client wireless per la modalità personale WPA2](#)

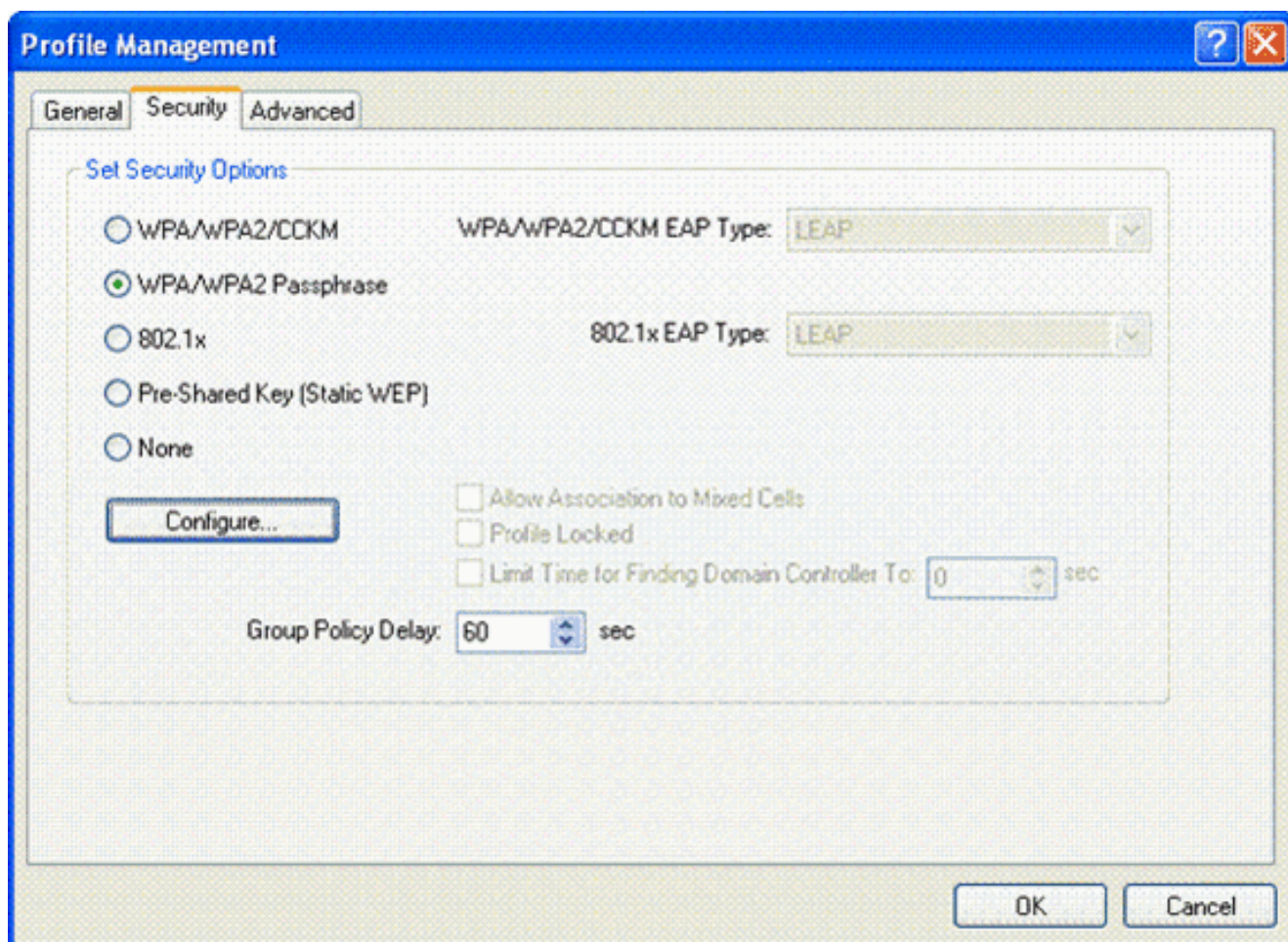
Il passaggio successivo consiste nel configurare il client wireless per la modalità di funzionamento WPA2-Personale.

Completare questa procedura per configurare il client wireless per la modalità WPA2-Personale:

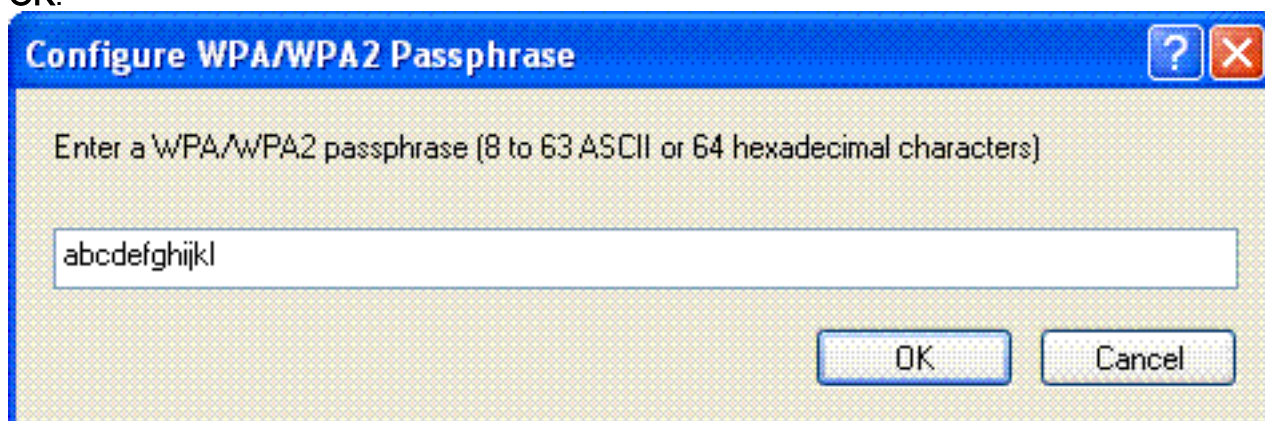
1. Dalla finestra Aironet Desktop Utility, fare clic su **Profile Management > New** (Gestione profili > Nuovo) per creare un profilo per l'utente WPA2-PSK WLAN.
2. Dalla finestra Gestione profili, fare clic sulla scheda **Generale** e configurare il Nome profilo, il Nome client e il Nome SSID come mostrato in questo esempio. Quindi fare clic su **OK**.



3. Fare clic sulla scheda **Security** (Sicurezza) e scegliere **WPA/WPA2 Passphrase** per abilitare la modalità di funzionamento WPA2-PSK. Per configurare la chiave già condivisa WPA-PSK, fare clic su **Configure** (Configura).



4. Immettere la chiave già condivisa e fare clic su **OK**.

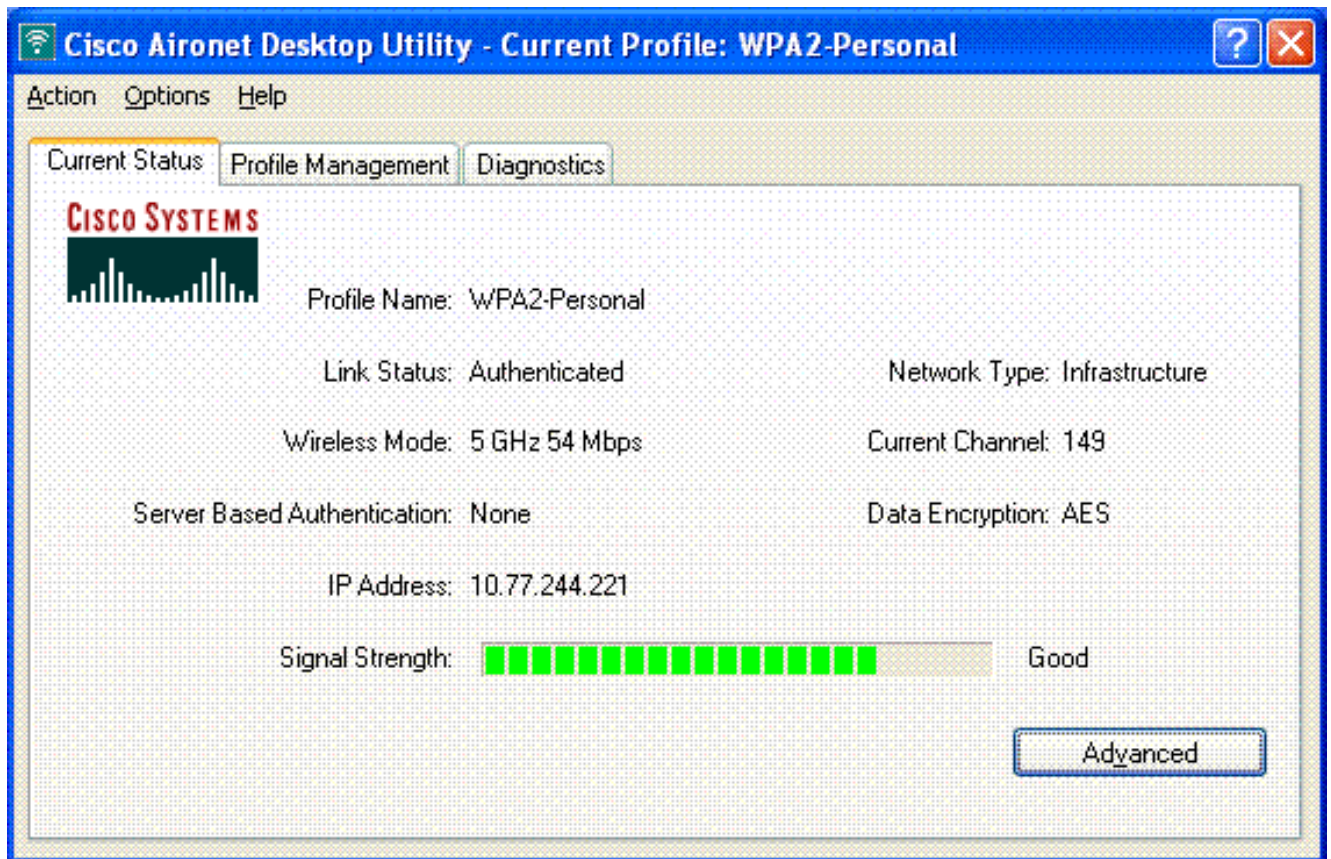


### Verifica modalità di funzionamento WPA2-Personale

Per verificare il corretto funzionamento della configurazione in modalità WPA2-Enterprise, completare i seguenti passaggi:

1. Dalla finestra Aironet Desktop Utility, selezionare il profilo **WPA2-Personal** e fare clic su **Activate** (Attiva) per attivare il profilo client wireless.
2. Una volta attivato il profilo, il client wireless si associa alla WLAN in seguito all'autenticazione. Ecco lo screenshot:





## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

I seguenti comandi di **debug** saranno utili per risolvere i problemi relativi alla configurazione:

**Nota:** consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di debug.

- **debug dot1x events enable:** abilita il debug di tutti gli eventi dot1x. Di seguito è riportato un esempio di output del comando debug basato su un'autenticazione riuscita: **Nota:** alcune delle righe di questo output sono state spostate in righe secondarie a causa dei limiti di spazio.

```
(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:** abilita il debug dei messaggi pacchetto 802.1x.
- **debug aaa events enable:** abilita l'output di debug di tutti gli eventi aaa.

## Informazioni correlate

- [WPA2 - Accesso protetto Wi-Fi 2](#)
- [Esempio di autenticazione EAP-FAST con i controller LAN wireless e la configurazione del server RADIUS esterno](#)
- [Esempio di configurazione dell'autenticazione EAP con i controller WLAN \(WLC\)](#)
- [Panoramica della configurazione WPA](#)
- [Supporto dei prodotti wireless](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).