

Esempio di configurazione del reindirizzamento della pagina iniziale del controller LAN wireless

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Installazione della rete](#)

[Configurazione](#)

[Passaggio 1. Configurare il WLC per l'autenticazione RADIUS tramite il server Cisco Secure ACS.](#)

[Passaggio 2. Configurare le WLAN per il reparto amministrativo e operativo.](#)

[Passaggio 3. Configurare Cisco Secure ACS in modo che supporti la funzione di reindirizzamento della pagina iniziale.](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare la funzione di reindirizzamento della pagina iniziale sui Wireless LAN Controller.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Conoscenza delle soluzioni di sicurezza LWAPP
- Informazioni su come configurare Cisco Secure ACS

Componenti usati

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

- Cisco serie 4400 Wireless LAN Controller (WLC) con firmware versione 5.0

- Cisco serie 1232 Light Weight Access Point (LAP)
- Cisco Aironet 802.a/b/g Adattatore client wireless con firmware versione 4.1
- Server Cisco Secure ACS con versione 4.1
- Qualsiasi server Web esterno di terze parti

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

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Premesse

Il reindirizzamento Web della pagina iniziale è una funzione introdotta con Wireless LAN Controller versione 5.0. Con questa funzione, l'utente viene reindirizzato a una particolare pagina Web dopo il completamento dell'autenticazione 802.1x. Il reindirizzamento si verifica quando l'utente apre un browser (configurato con una home page predefinita) o tenta di accedere a un URL. Al termine del reindirizzamento alla pagina Web, l'utente ha accesso completo alla rete.

È possibile specificare la pagina di reindirizzamento nel server RADIUS (Remote Authentication Dial-In User Service). Il server RADIUS deve essere configurato in modo da restituire l'attributo Cisco av-pair url-redirect RADIUS al controller LAN wireless dopo la riuscita autenticazione 802.1x.

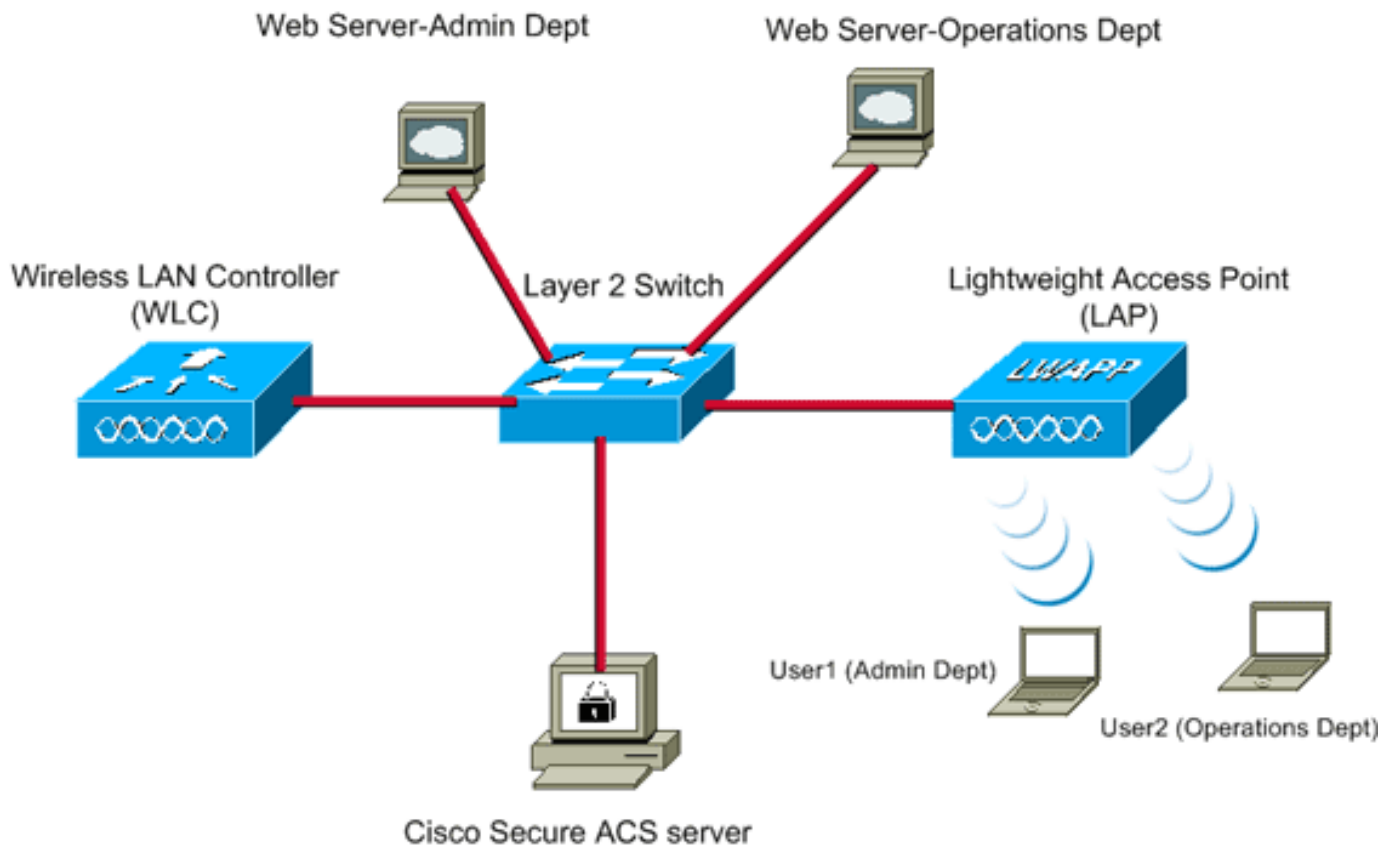
La funzione di reindirizzamento Web della pagina iniziale è disponibile solo per le WLAN configurate per la sicurezza di layer 2 802.1x o WPA/WPA2.

Installazione della rete

Nell'esempio, un Cisco 4404 WLC e un Cisco serie 1232 LAP sono connessi tramite uno switch di layer 2. Anche il server Cisco Secure ACS (che agisce come server RADIUS esterno) è connesso allo stesso switch. Tutti i dispositivi si trovano nella stessa subnet.

Il LAP è inizialmente registrato sul controller. È necessario creare due WLAN: una per gli utenti del **reparto di amministrazione** e l'altra per gli utenti del **reparto operazioni**. Entrambe le LAN wireless utilizzano WPA2/ AES (per l'autenticazione viene utilizzato EAP-FAST). Entrambe le WLAN utilizzano la funzione di reindirizzamento della pagina iniziale per reindirizzare gli utenti agli URL della home page appropriati (su server Web esterni).

Nel documento viene usata questa impostazione di rete:



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

La sezione successiva spiega come configurare i dispositivi per questa installazione.

[Configurazione](#)

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

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

Per configurare i dispositivi in modo che utilizzino la funzionalità di reindirizzamento della pagina iniziale, completare la procedura seguente:

1. [Configurare il WLC per l'autenticazione RADIUS tramite il server Cisco Secure ACS.](#)
2. [Configurare le WLAN per i reparti Admin e Operations.](#)
3. [Configurare Cisco Secure ACS in modo che supporti la funzione di reindirizzamento della pagina iniziale.](#)

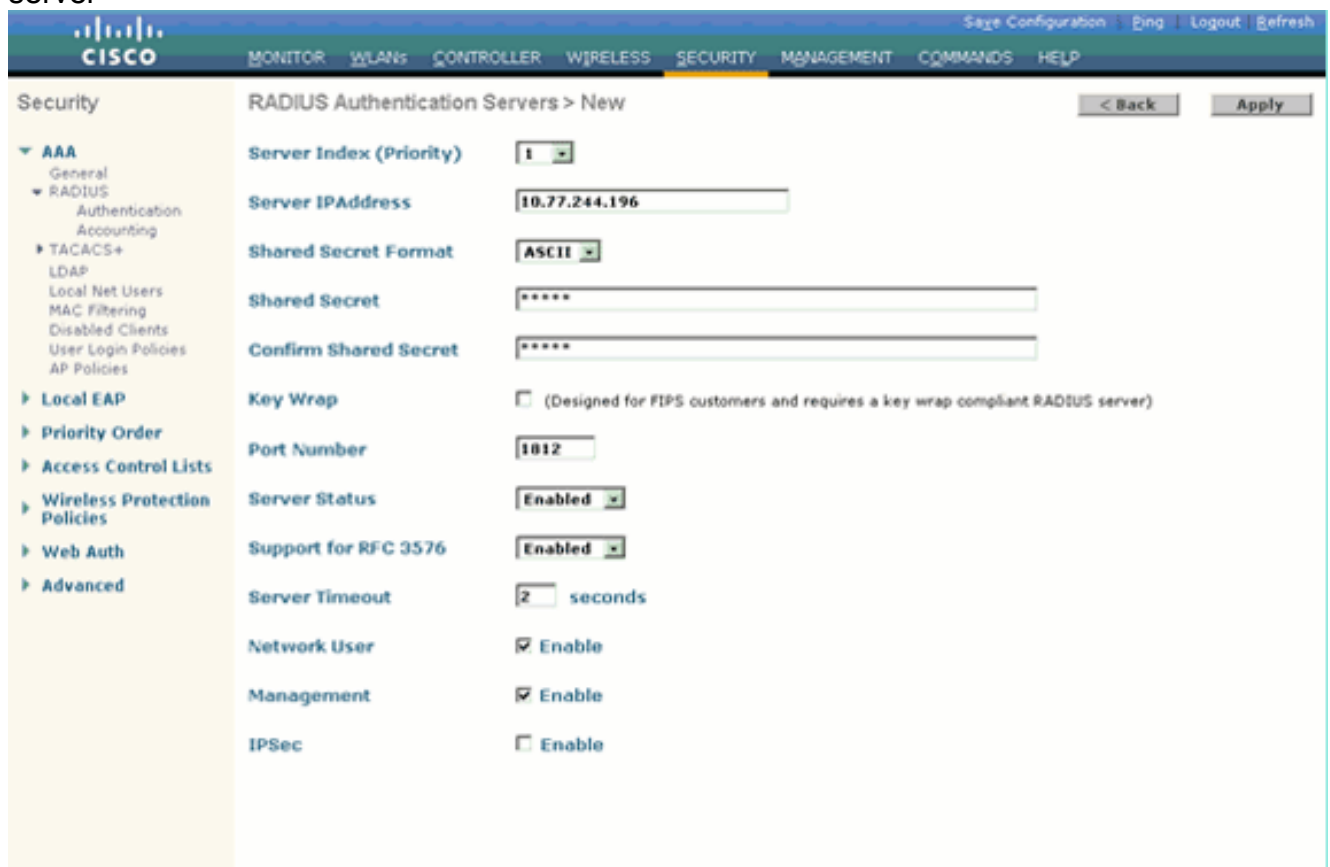
[Passaggio 1. Configurare il WLC per l'autenticazione RADIUS tramite il server](#)

[Cisco Secure ACS.](#)

Per inoltrare le credenziali dell'utente a un server RADIUS esterno, è necessario configurare il WLC.

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

1. Selezionare **Security** (Sicurezza) e **RADIUS Authentication** (Autenticazione RADIUS) dall'interfaccia utente del controller per visualizzare la pagina Server di autenticazione RADIUS.
2. Per definire un server RADIUS, fare clic su **New** (Nuovo).
3. Definire i parametri del server RADIUS nella pagina Server di autenticazione RADIUS > Nuovo. Questi parametri includono: Indirizzo IP server RADIUS, Segreto condiviso, Numero porta, Stato server



The screenshot shows the Cisco Secure ACS configuration page for RADIUS Authentication Servers. The page title is "RADIUS Authentication Servers > New". The left sidebar shows the navigation menu with "Security" 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

In questo documento viene usato il server ACS con indirizzo IP 10.77.244.196.

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

[Passaggio 2. Configurare le WLAN per il reparto amministrativo e operativo.](#)

In questo passaggio vengono configurate le due WLAN (una per il reparto Amministratori e l'altra per il reparto Operazioni) che i client utilizzeranno per connettersi alla rete wireless.

L'SSID WLAN per il reparto Admin sarà *Admin*. L'SSID WLAN per il reparto operazioni sarà *Operations* (Operazioni).

Usare l'autenticazione EAP-FAST per abilitare WPA2 come meccanismo di sicurezza di layer 2 sia sulle WLAN che sulla funzione Web policy - Splash Page Web Redirect come metodo di

sicurezza di layer 3.

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).

The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The left sidebar shows 'WLANs' with a sub-menu 'Advanced'. The main content area is titled 'WLANs > New' and contains the following fields:

Type	WLAN
Profile Name	Admin
WLAN SSID	Admin

Buttons for '< Back' and 'Apply' are visible in the top right corner.

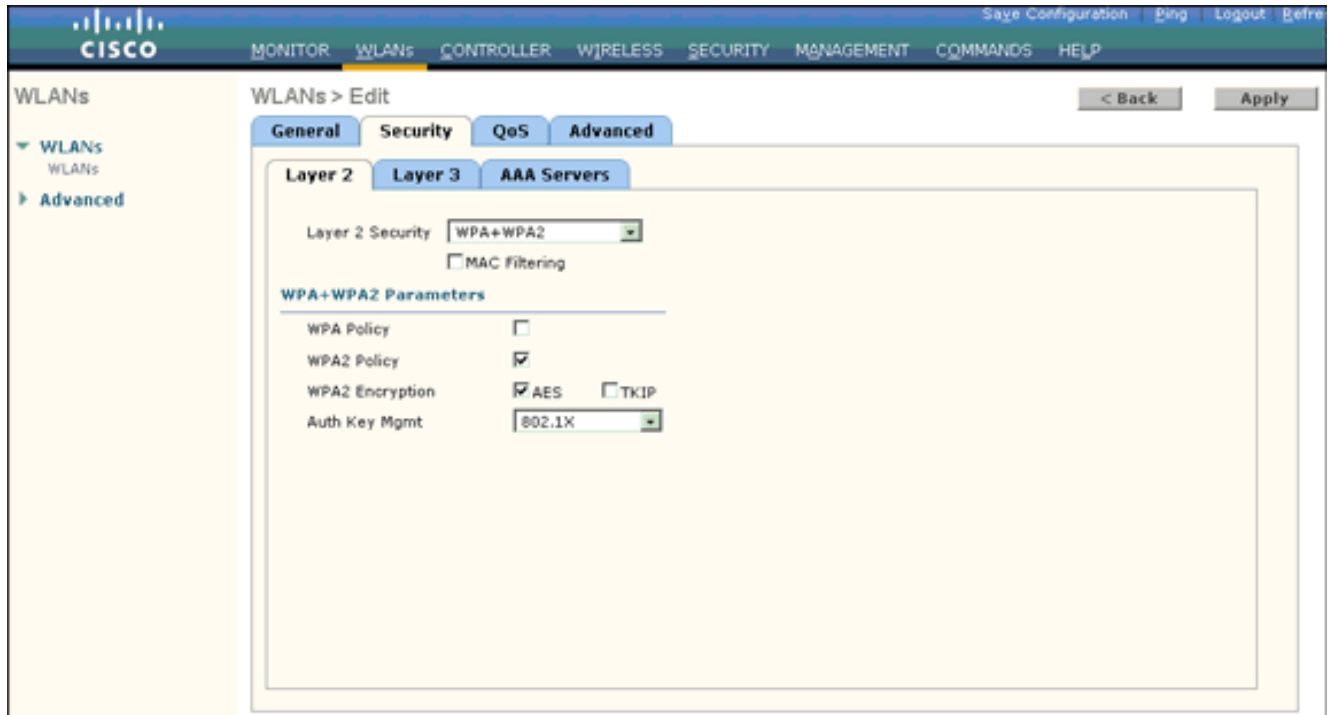
3. Immettere il nome dell'SSID della WLAN e il nome del profilo nella pagina WLAN > Nuovo.
4. Fare clic su **Apply** (Applica).
5. Innanzitutto creiamo la WLAN per il reparto amministrativo. Dopo aver creato una nuova WLAN, viene visualizzata la pagina WLAN > Modifica per la nuova WLAN. In questa pagina 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.
6. Per abilitare la WLAN, in Criteri generali selezionare la casella di controllo **Stato**.

The screenshot shows the Cisco WLAN configuration interface for editing an existing WLAN. The top navigation bar is the same as in the previous screenshot. The left sidebar shows 'WLANs' with a sub-menu 'Advanced'. The main content area is titled 'WLANs > Edit' and contains the following fields:

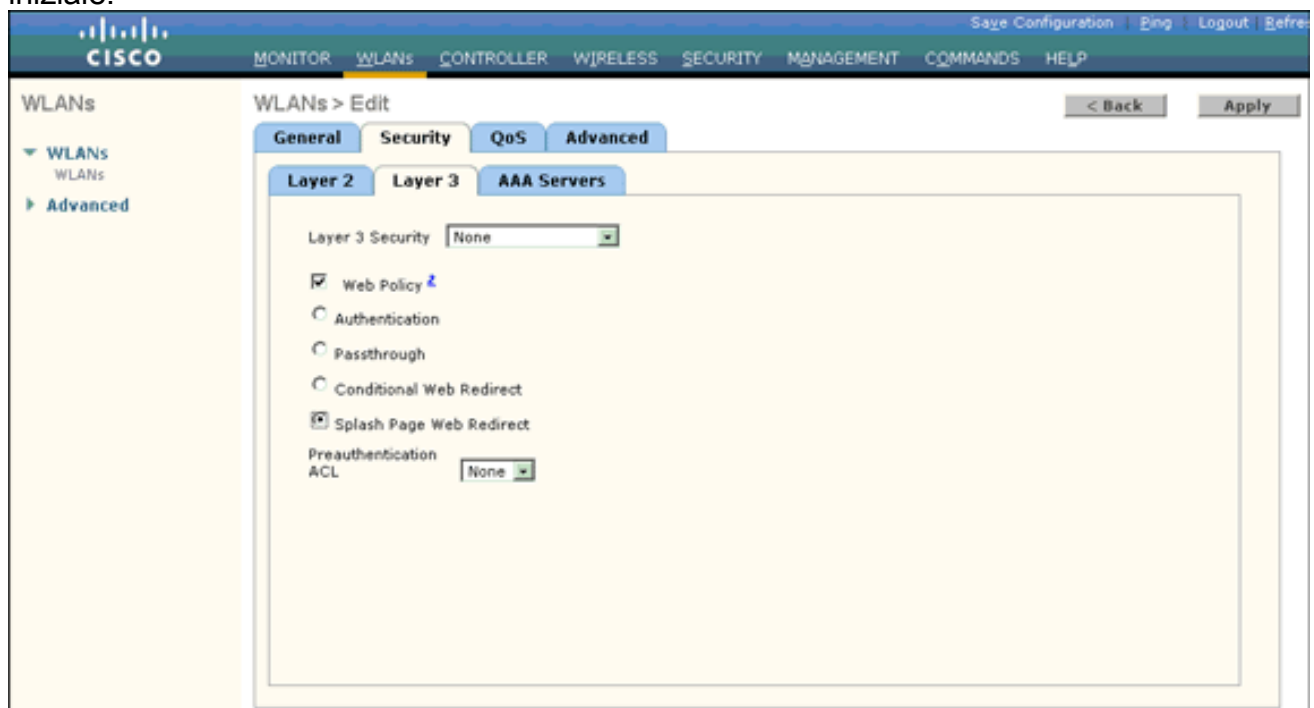
Profile Name	Admin
Type	WLAN
SSID	Admin
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	Splash-Page-Web-Redirect[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface	admin
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

Buttons for '< Back' and 'Apply' are visible in the top right corner.

7. Fare clic sulla scheda **Protezione** e quindi sulla scheda **Layer 2**.
8. Selezionare **WPA+WPA2** dall'elenco a discesa Protezione di layer 2. Questo passaggio consente di abilitare l'autenticazione WPA per la WLAN.
9. In Parametri WPA+WPA2 selezionare le caselle di controllo **Criterio WPA2** e **Crittografia AES**.

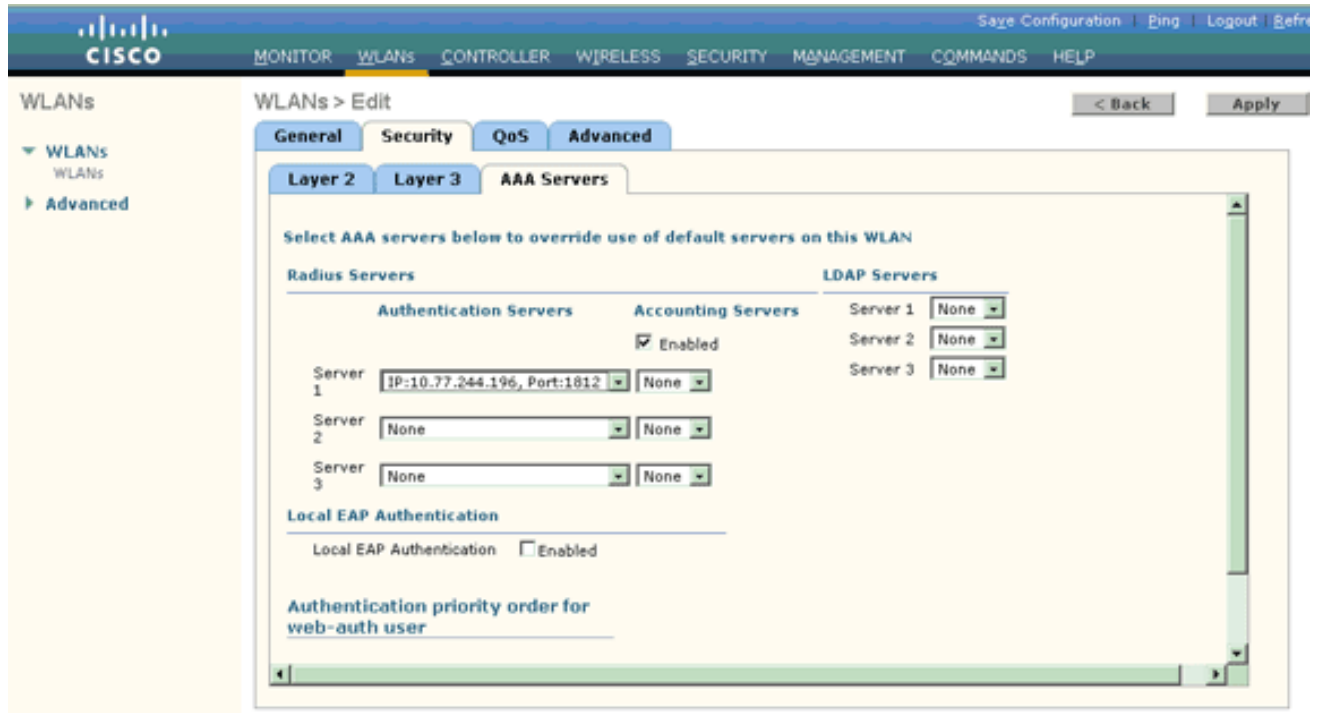


10. Selezionare **802.1x** dall'elenco a discesa Auth Key Mgmt. Questa opzione abilita WPA2 con autenticazione 802.1x/EAP e crittografia AES per la WLAN.
11. Fare clic sulla scheda **Protezione di livello 3**.
12. Selezionare la casella **Criteri Web**, quindi fare clic sul pulsante di opzione **Reindirizzamento Web pagina iniziale**. Questa opzione attiva la funzione Web Redirect della pagina iniziale.



13. Fare clic sulla scheda **Server AAA**.
14. In Server di autenticazione scegliere l'indirizzo IP del server appropriato dall'elenco a discesa Server

1.



Nell'esempio, 10.77.244.196 viene usato come server RADIUS.

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

16. Ripetere i passaggi da 2 a 15 per creare la WLAN per il reparto operazioni. Nella pagina WLAN sono elencate le due WLAN create.



I criteri di protezione includono il reindirizzamento della pagina iniziale.

[Passaggio 3. Configurare Cisco Secure ACS in modo che supporti la funzione di reindirizzamento della pagina iniziale.](#)

Il passaggio successivo consiste nella configurazione del server RADIUS per questa funzionalità. Il server RADIUS deve eseguire l'autenticazione EAP-FAST per convalidare le credenziali del client e, se l'autenticazione ha esito positivo, per reindirizzare l'utente all'URL (sul server Web esterno) specificato nell'attributo RADIUS di **reindirizzamento URL** a coppia av Cisco.

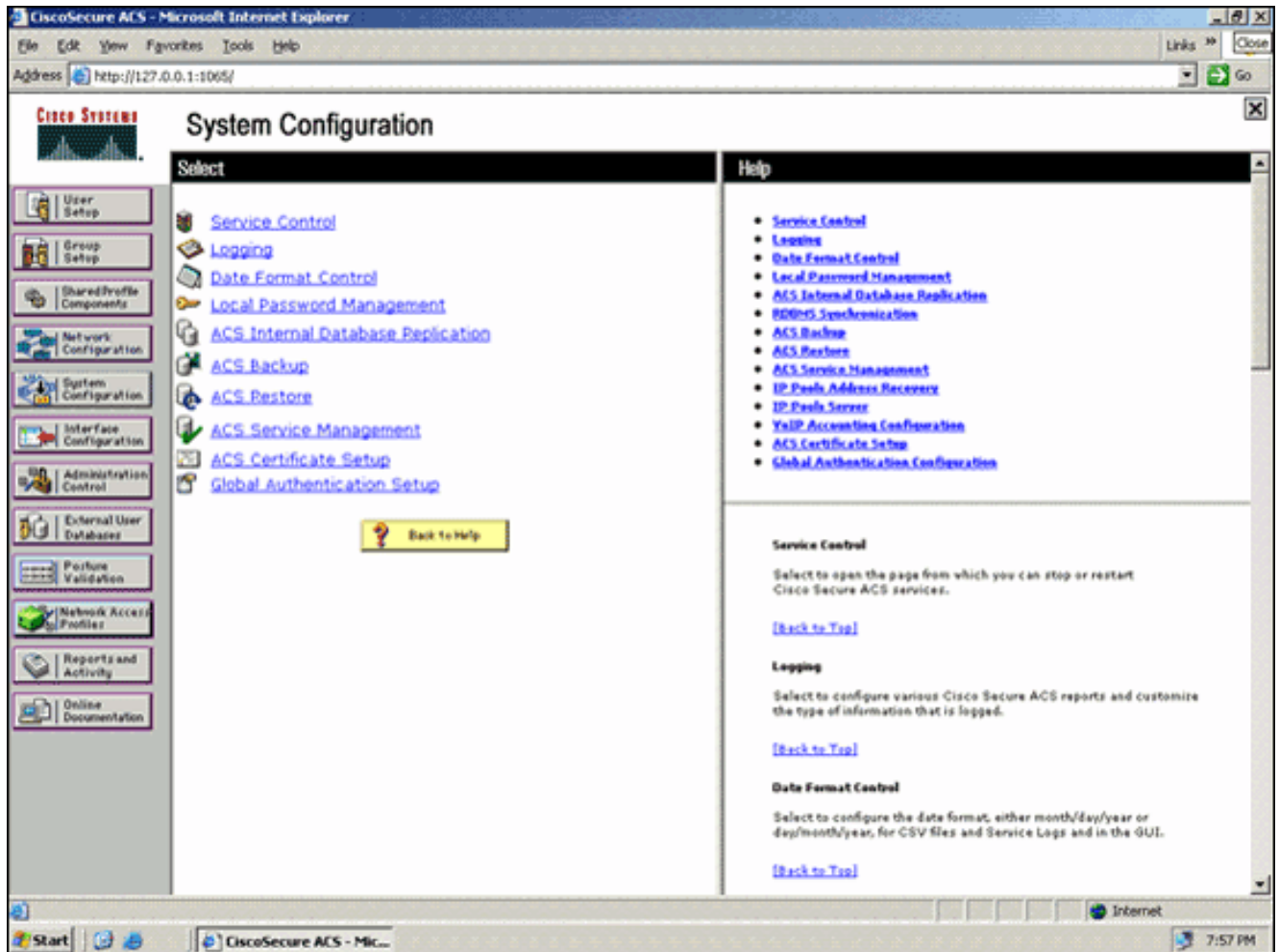
Configurazione di Cisco Secure ACS per l'autenticazione EAP-FAST

Nota: in questo documento si presume che il controller LAN wireless sia stato aggiunto al Cisco

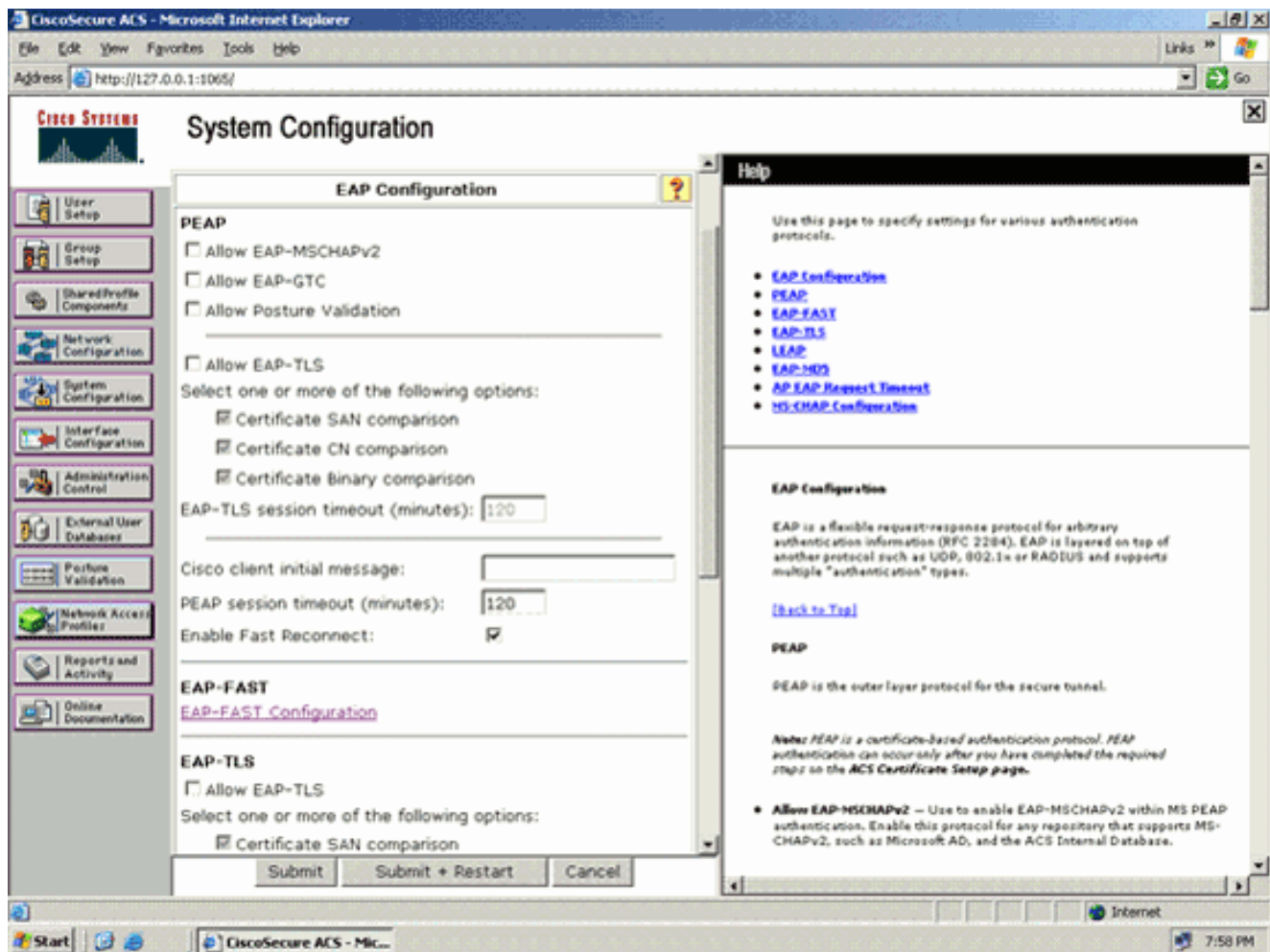
Secure ACS come client AAA.

Completare questa procedura per configurare l'autenticazione EAP-FAST nel server RADIUS:

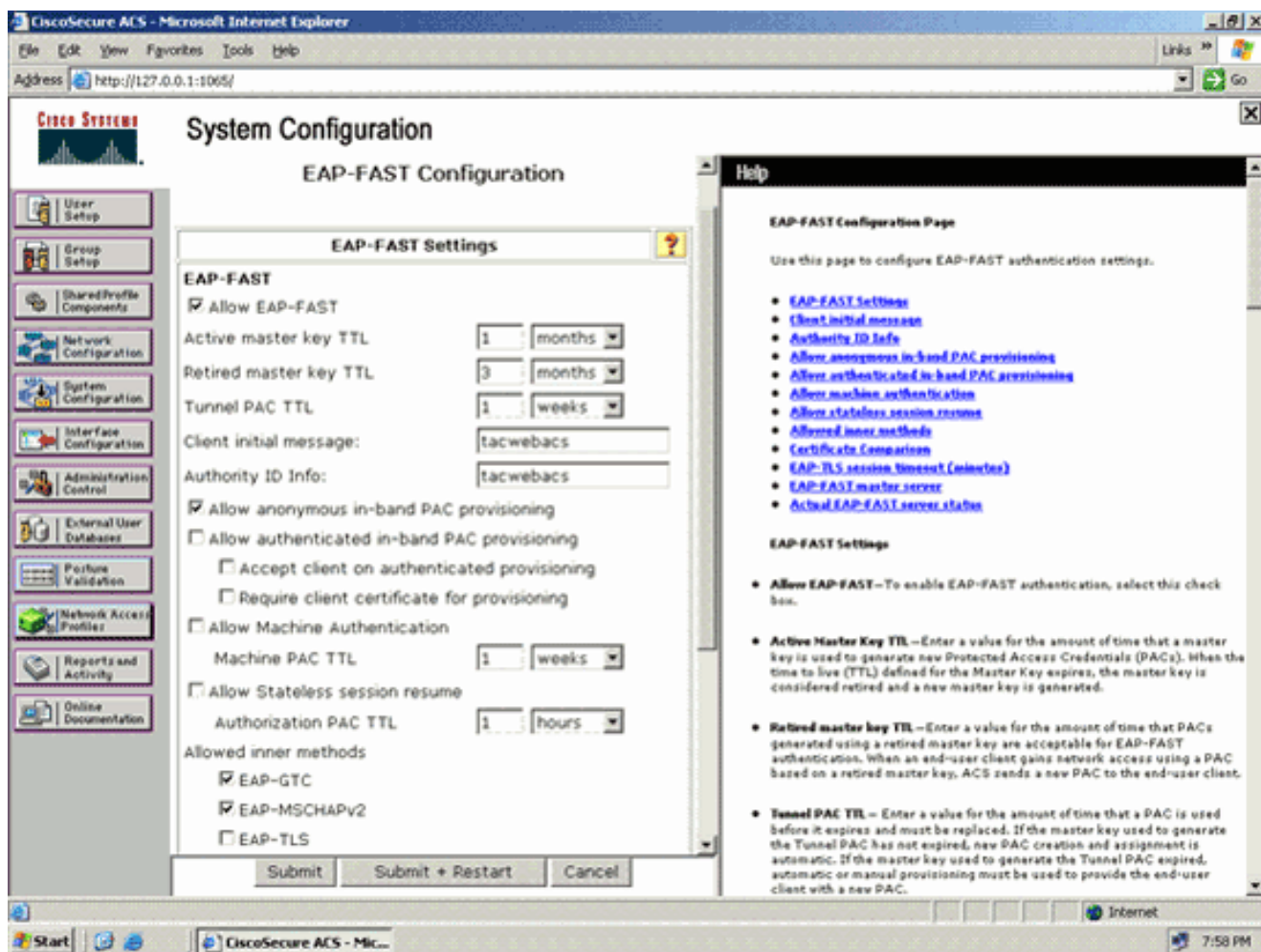
1. Fare clic su **Configurazione del sistema** dall'interfaccia utente del server RADIUS, quindi scegliere **Configurazione autenticazione globale** dalla pagina Configurazione del sistema.



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



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



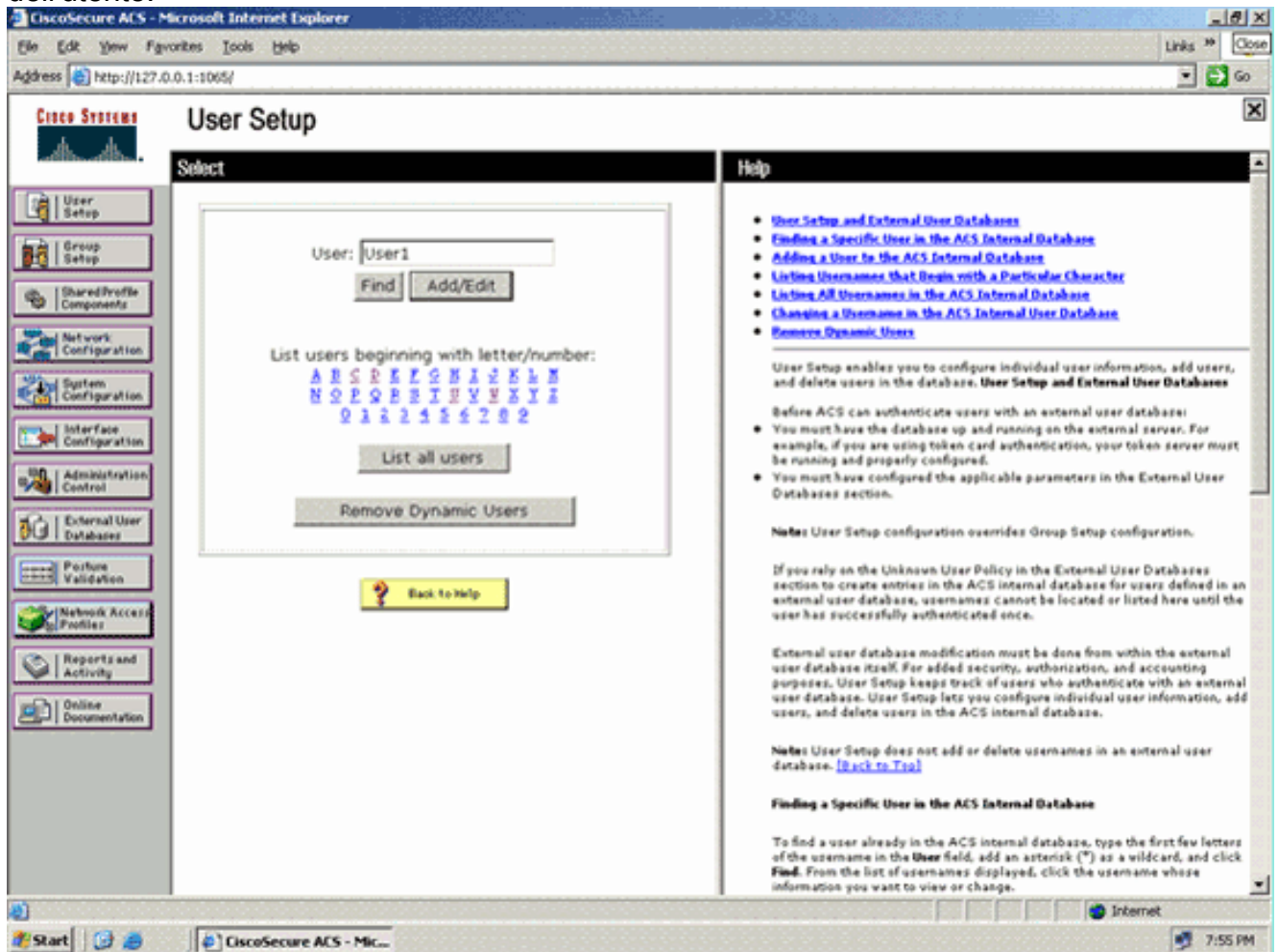
4. Configurare i valori TTL (Time-to-Live) della chiave master attiva/ritirata in base alle esigenze oppure impostarli sul valore predefinito, come illustrato in questo esempio. Il campo Authority ID Info (Informazioni ID autorità) rappresenta l'identità testuale del server ACS, che un utente finale 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. L'opzione *Allowed inner methods* determina i metodi EAP interni che 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).
7. Fare clic su **Invia**. **Nota:** per informazioni dettagliate ed esempi su come configurare EAP FAST con il provisioning in-band PAC anonimo e il provisioning in-band autenticato, fare riferimento all'[esempio di autenticazione EAP-FAST con i controller LAN wireless e la configurazione del server RADIUS esterno](#).

Configurare il database utente e definire l'attributo RADIUS di reindirizzamento URL

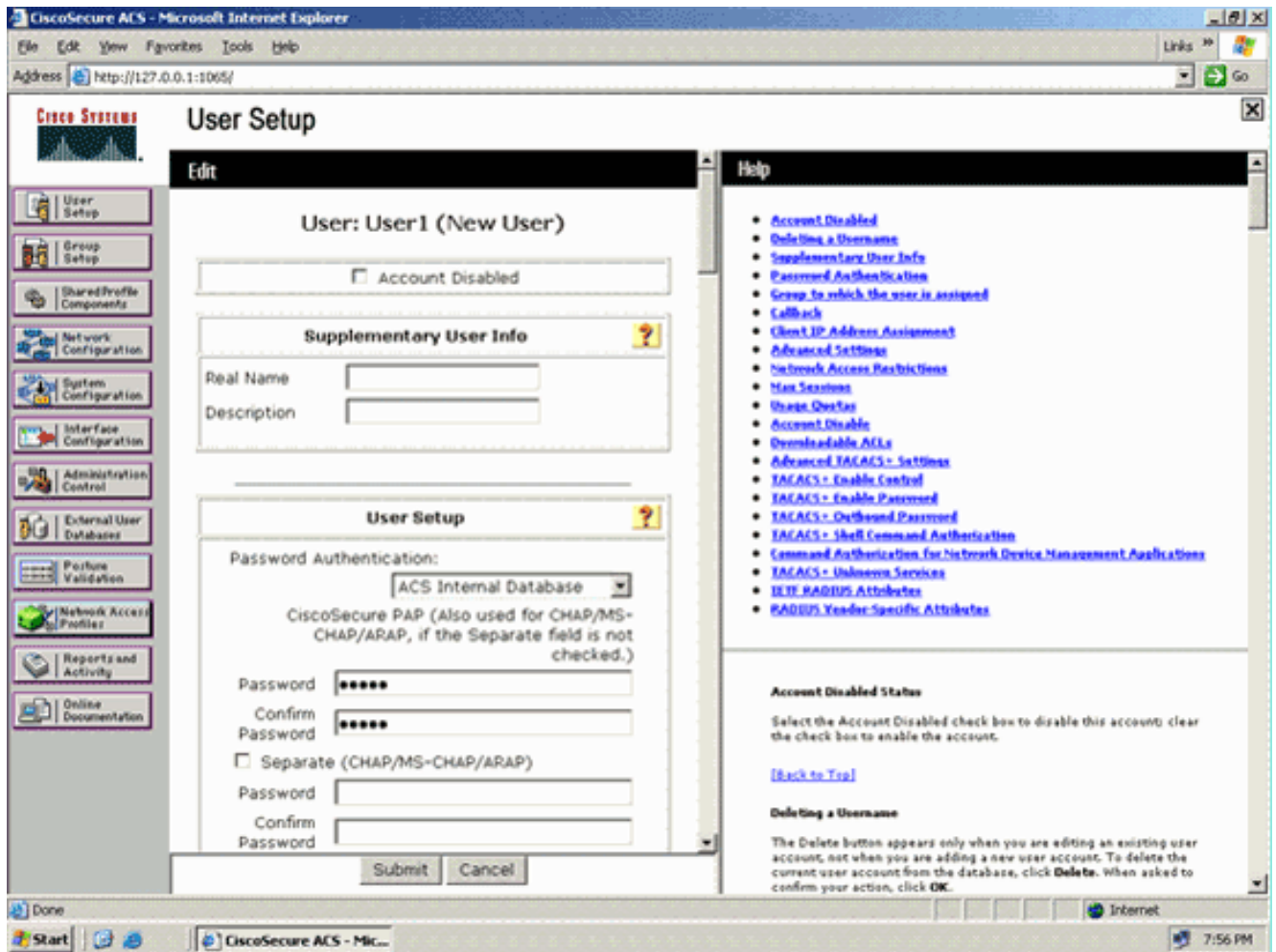
In questo esempio il nome utente e la password del client wireless vengono configurati rispettivamente come Utente1 e Utente1.

Per creare un database utenti, effettuare i seguenti passaggi:

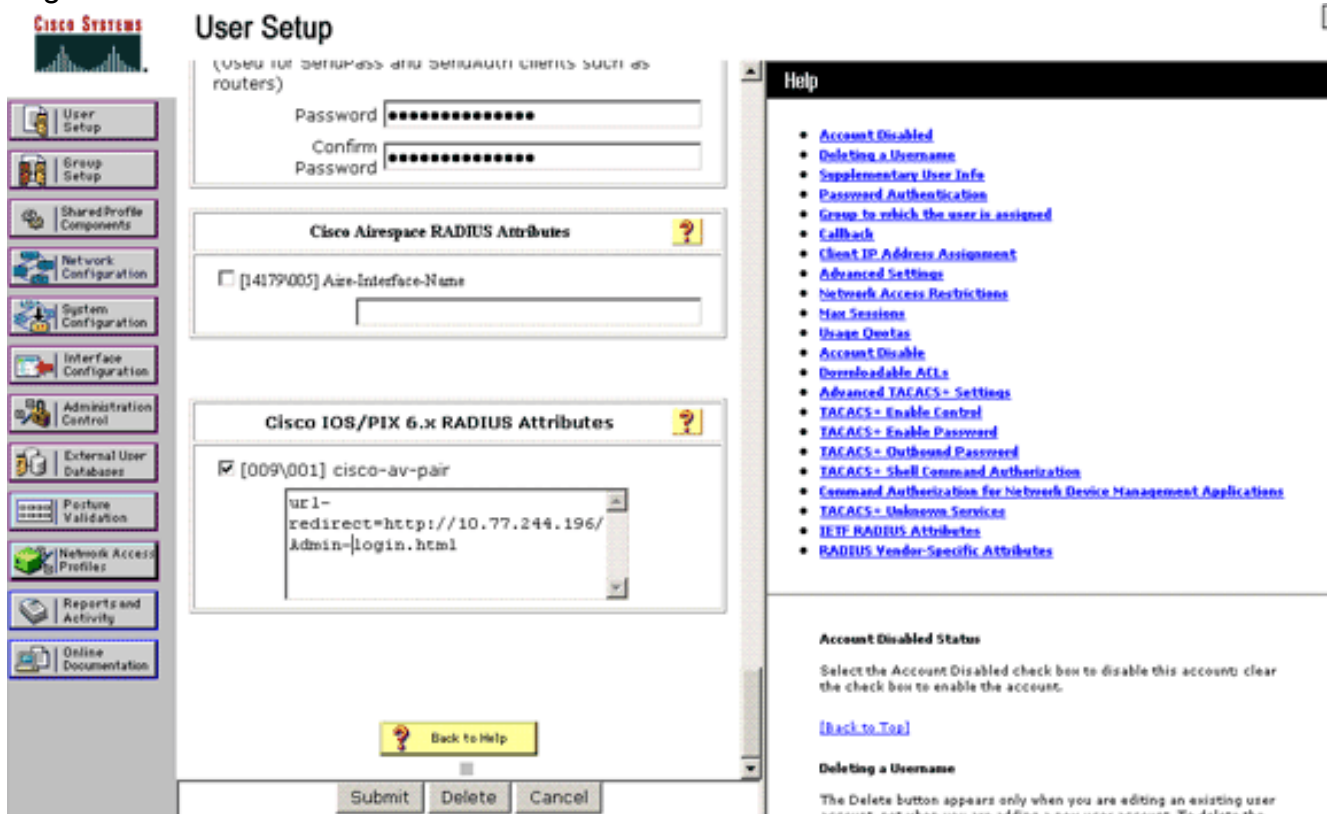
1. Dalla GUI di ACS nella barra di navigazione, scegliere **User Setup** (Configurazione utente).
2. Creare un nuovo utente senza fili e quindi fare clic su **Aggiungi/Modifica** per accedere alla pagina Modifica dell'utente.



3. Nella pagina Modifica della configurazione utente, 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.



4. Scorrere la pagina verso il basso per modificare gli attributi RADIUS.
5. Selezionare la casella di controllo [009\001] cisco-av-pair.
6. Immettere queste coppie di av Cisco nella casella di modifica [009\001] cisco-av-pair per specificare l'URL a cui l'utente viene reindirizzato: url-redirect=http://10.77.244.196/Admin-Login.html



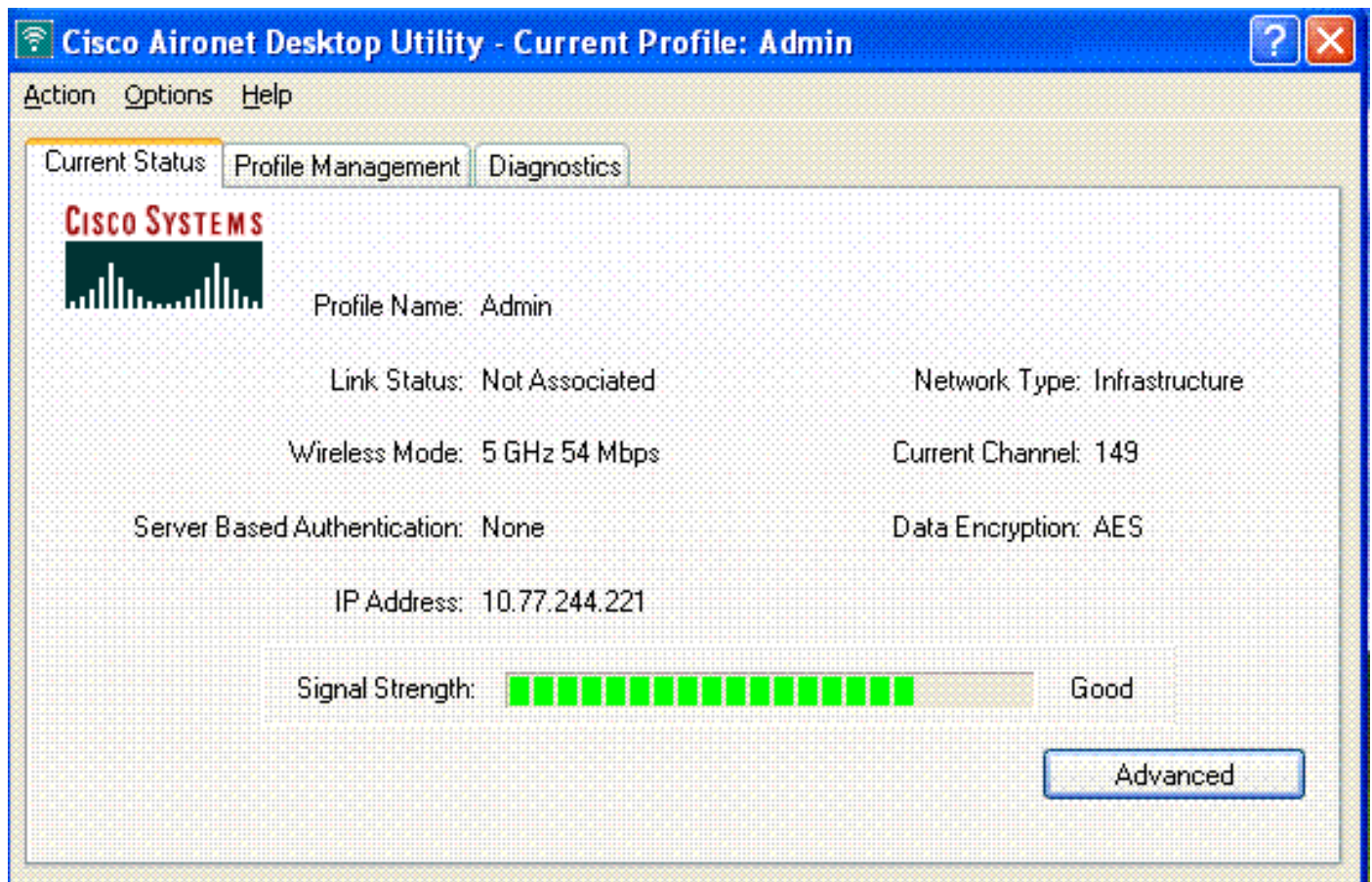
Questa è la home page degli utenti del reparto di amministrazione.

7. Fare clic su **Invia**.
8. Ripetere questa procedura per aggiungere User2 (utente del reparto operazioni).
9. Ripetere i passaggi da 1 a 6 per aggiungere al database altri utenti del reparto di amministrazione e del reparto operazioni. **Nota:** gli attributi RADIUS possono essere configurati a livello di utente o di gruppo su Cisco Secure ACS.

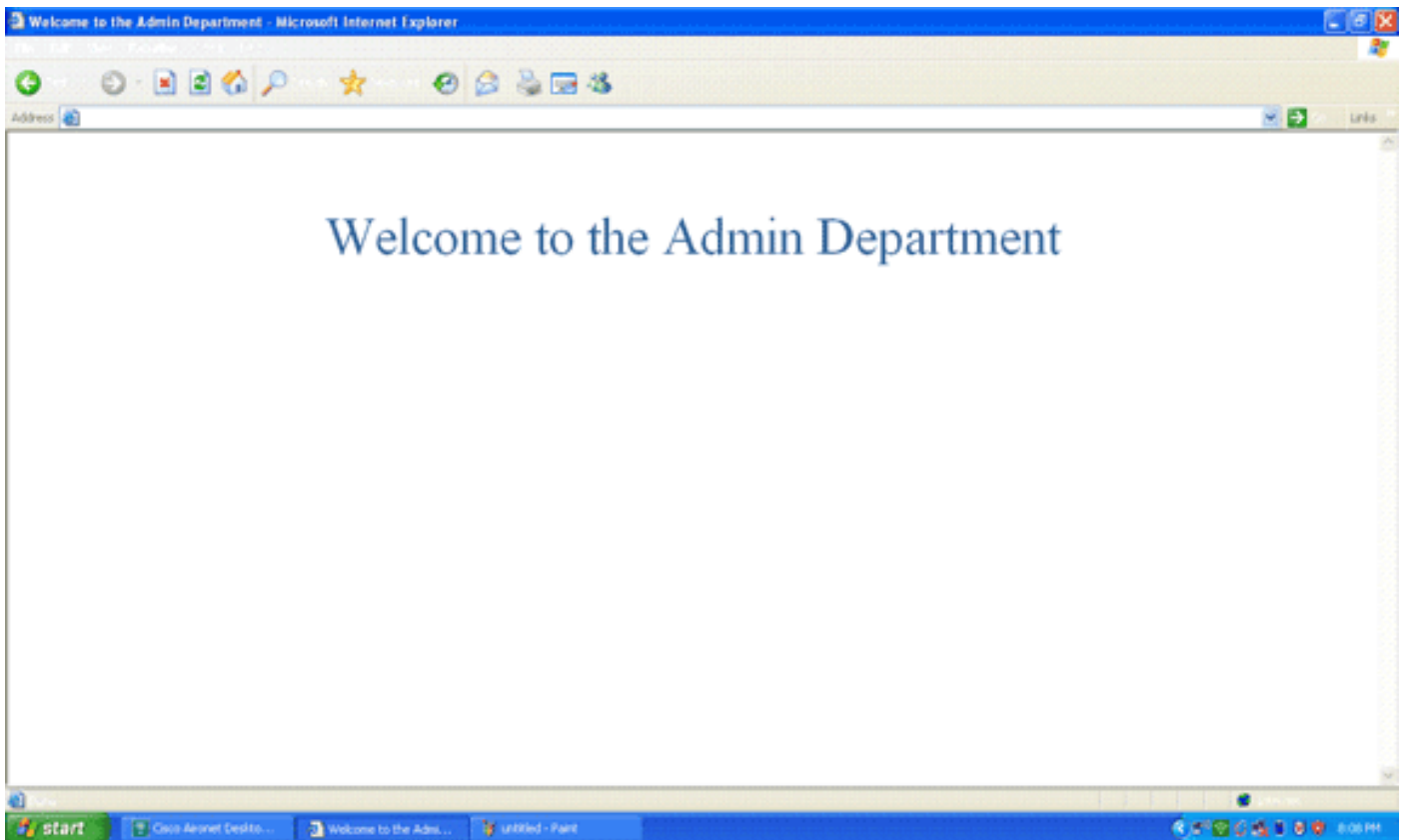
Verifica

Per verificare la configurazione, associare un client WLAN del reparto di amministrazione e del reparto operazioni alle WLAN appropriate.

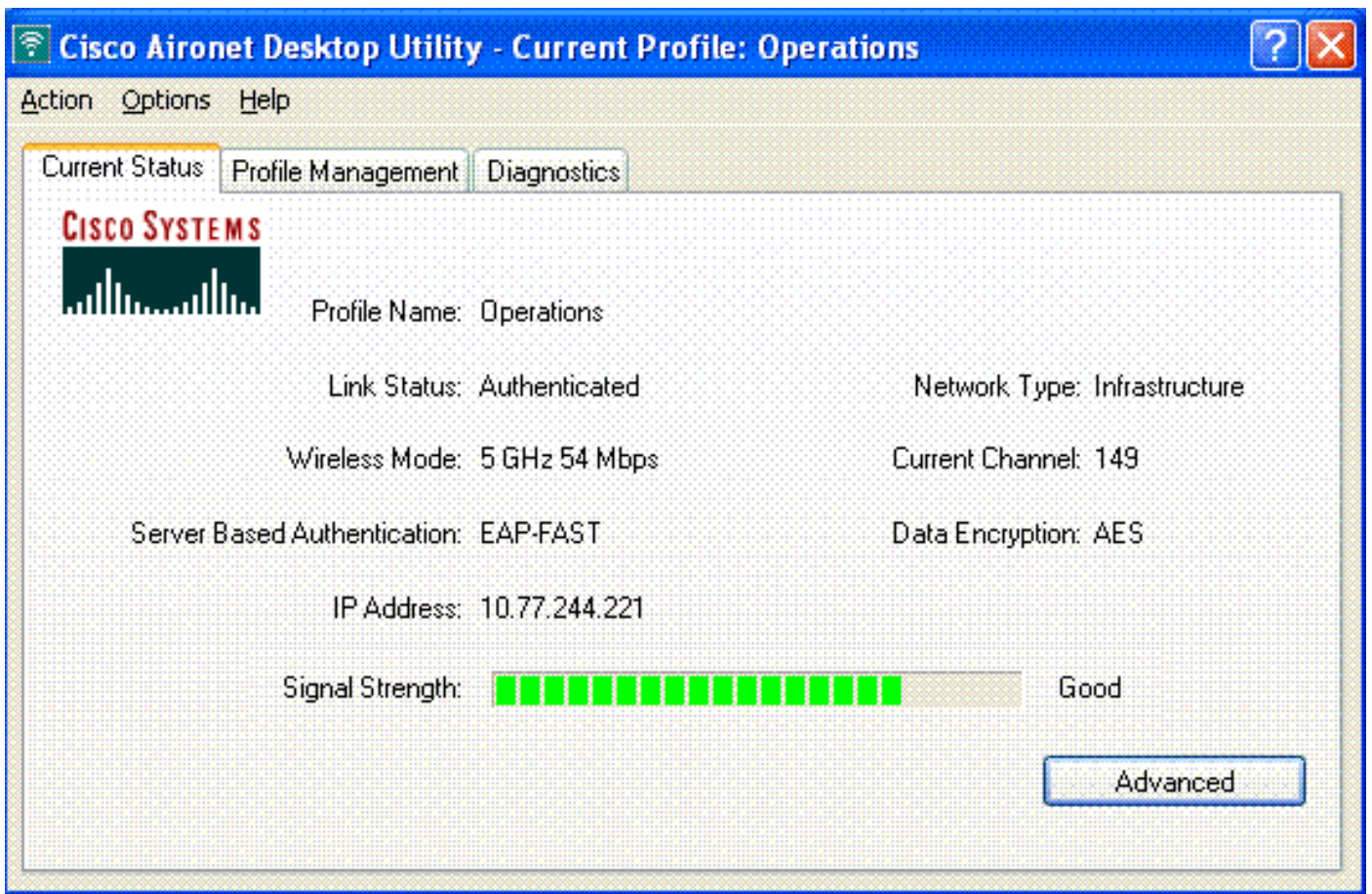
Quando un utente del reparto di amministrazione si connette all'amministratore LAN wireless, all'utente vengono richieste credenziali 802.1x (credenziali EAP-FAST nel caso specifico). Una volta che l'utente ha fornito le credenziali, il WLC le passa al server Cisco Secure ACS. Il server Cisco Secure ACS convalida le credenziali dell'utente a fronte del database e, se l'autenticazione ha esito positivo, restituisce l'attributo url-redirect al controller LAN wireless. Autenticazione completata in questa fase.

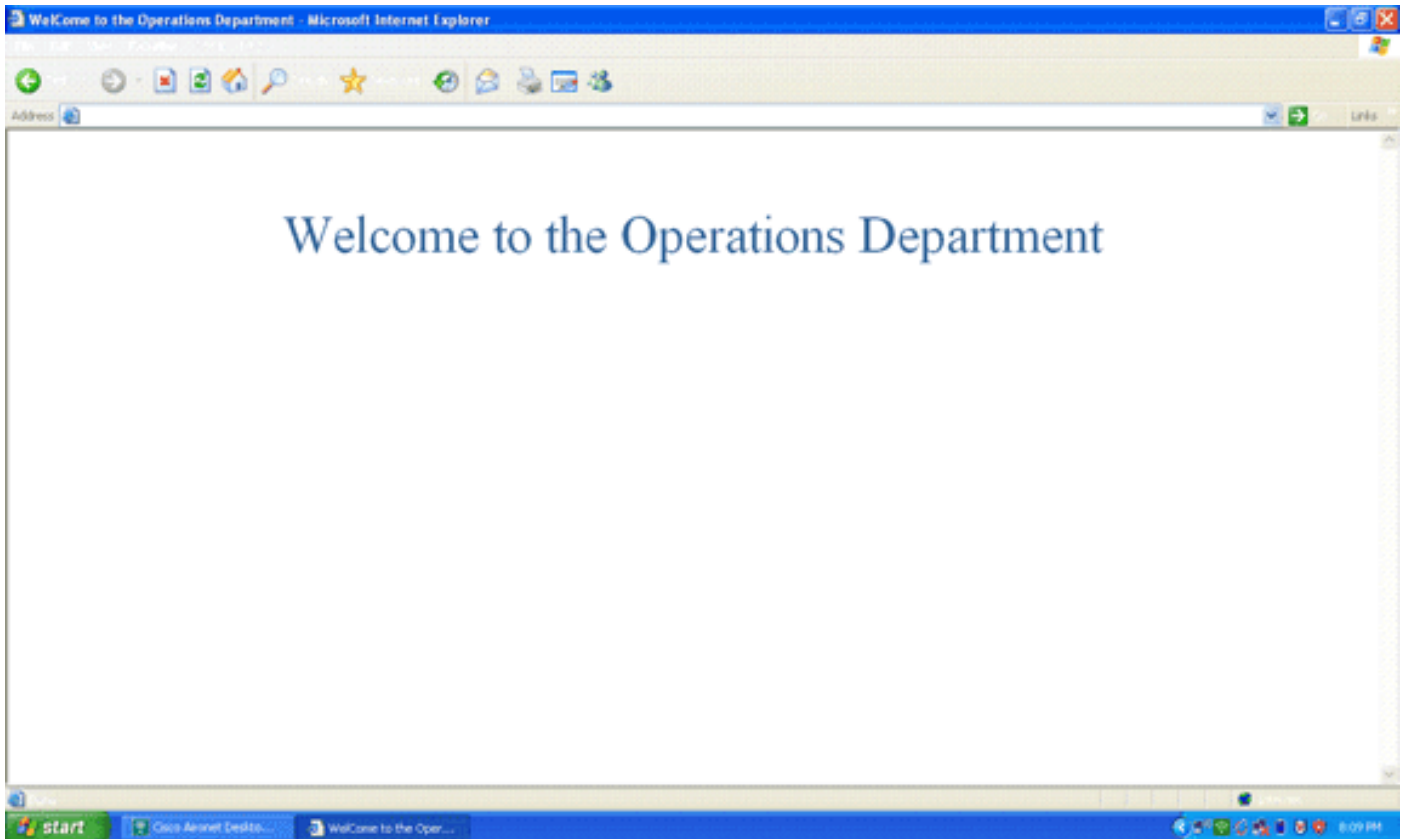


Quando l'utente apre un browser Web, viene reindirizzato all'URL della home page del reparto Admin. (Questo URL viene restituito al WLC tramite l'attributo cisco-av-pair). Dopo il reindirizzamento, l'utente ha accesso completo alla rete. Ecco gli screenshot:



Le stesse sequenze di eventi si verificano quando un utente del reparto operazioni si connette alle operazioni WLAN.





Risoluzione dei problemi

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

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

Per risolvere i problemi relativi alla configurazione, è possibile utilizzare i comandi seguenti.

- **show wlan id_wlan:** visualizza lo stato delle funzionalità di reindirizzamento Web per una particolare WLAN. Di seguito è riportato un esempio:

```
WLAN Identifier..... 1
Profile Name..... Admin
Network Name (SSID)..... Admin
...
Web Based Authentication..... Disabled
Web-Passthrough..... Disabled
Conditional Web Redirect..... Disabled
Splash-Page Web Redirect..... Enabled
```

- **debug dot1x events enable:** abilita il debug dei messaggi pacchetto 802.1x. Di seguito è riportato un esempio:

```
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP Request from AAA to
mobile 00:40:96:ac:dd:05 (EAP Id 16)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAPOL EAPPKT from
mobile 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAP Response from
mobile 00:40:96:ac:dd:05 (EAP Id 16, EAP Type 43)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Processing Access-Challenge for
mobile 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Setting re-auth timeout to 1800
```

```

seconds, got from WLAN config.
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Station 00:40:96:ac:dd:05
setting dot1x reauth timeout = 1800
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Creating a new PMK Cache Entry
for station 00:40:96:ac:dd:05 (RSN 2)
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Adding BSSID 00:1c:58:05:e9:cf
to PMKID cache for station 00:40:96:ac:dd:05
Fri Feb 29 10:27:16 2008: New PMKID: (16)
Fri Feb 29 10:27:16 2008:          [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
fb fa 8e 3c
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Disabling re-auth since PMK
lifetime can take care of same.
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP-Success to mobile
00:40:96:ac:dd:05 (EAP Id 17)
Fri Feb 29 10:27:16 2008: Including PMKID in M1 (16)
Fri Feb 29 10:27:16 2008:          [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca
fb fa 8e 3c
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAPOL-Key Message to
mobile 00:40:96:ac:dd:05
state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received Auth Success while
in Authenticating state for mobile 00:40:96:ac:dd:05

```

- **debug aaa events enable:** abilita l'output di debug di tutti gli eventi aaa. Di seguito è riportato un esempio:

```

Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
Authentication Packet (id 103) to 10.77.244.196:1812, proxy state
00:40:96:ac:dd:05-00:00
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=11
Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=11
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Challenge received from
RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
Authentication Packet (id 104) to 10.77.244.196:1812, proxy state
00:40:96:ac:dd:05-00:00
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=2
Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=2
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Accept received from
RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 AAA Override Url-Redirect
'http://10.77.244.196/Admin-login.html' set
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Applying new AAA override for
station 00:40:96:ac:dd:05
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Override values for station
00:40:96:ac:dd:05
source: 4, valid bits: 0x0
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
dataAvgC: -1, rTAVgC: -1, dataBurstC: -1, rTimeBurstC: -1
vlanIfName: '', aclName: '

```

[Informazioni correlate](#)

- [Guida alla configurazione di Cisco Wireless LAN Controller, versione 5.0](#)
- [Esempio di configurazione dell'autenticazione Web del controller LAN wireless](#)
- [Esempio di configurazione dell'autenticazione Web esterna con i controller LAN wireless](#)
- [Pagina di supporto 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).