

# Autenticazione Web esterna tramite server RADIUS

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Convenzioni](#)

[Autenticazione Web esterna](#)

[Configurare il WLC](#)

[Configurazione del WLC per Cisco Secure ACS](#)

[Configurazione della WLAN sul WLC per l'autenticazione Web](#)

[Configurare le informazioni sul server Web sul WLC](#)

[Configurazione di Cisco Secure ACS](#)

[Configurazione delle informazioni utente su Cisco Secure ACS](#)

[Configurazione delle informazioni WLC su Cisco Secure ACS](#)

[Processo di autenticazione client](#)

[Configurazione client](#)

[Processo di login client](#)

[Verifica](#)

[Verifica ACS](#)

[Verifica WLC](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Informazioni correlate](#)

## [Introduzione](#)

Questo documento spiega come eseguire l'autenticazione Web esterna utilizzando un server RADIUS esterno.

## [Prerequisiti](#)

### [Requisiti](#)

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

- Conoscenze base della configurazione dei Lightweight Access Point (LAP) e dei Cisco WLC

- Informazioni su come configurare un server Web esterno
- Informazioni su come configurare Cisco Secure ACS

## Componenti usati

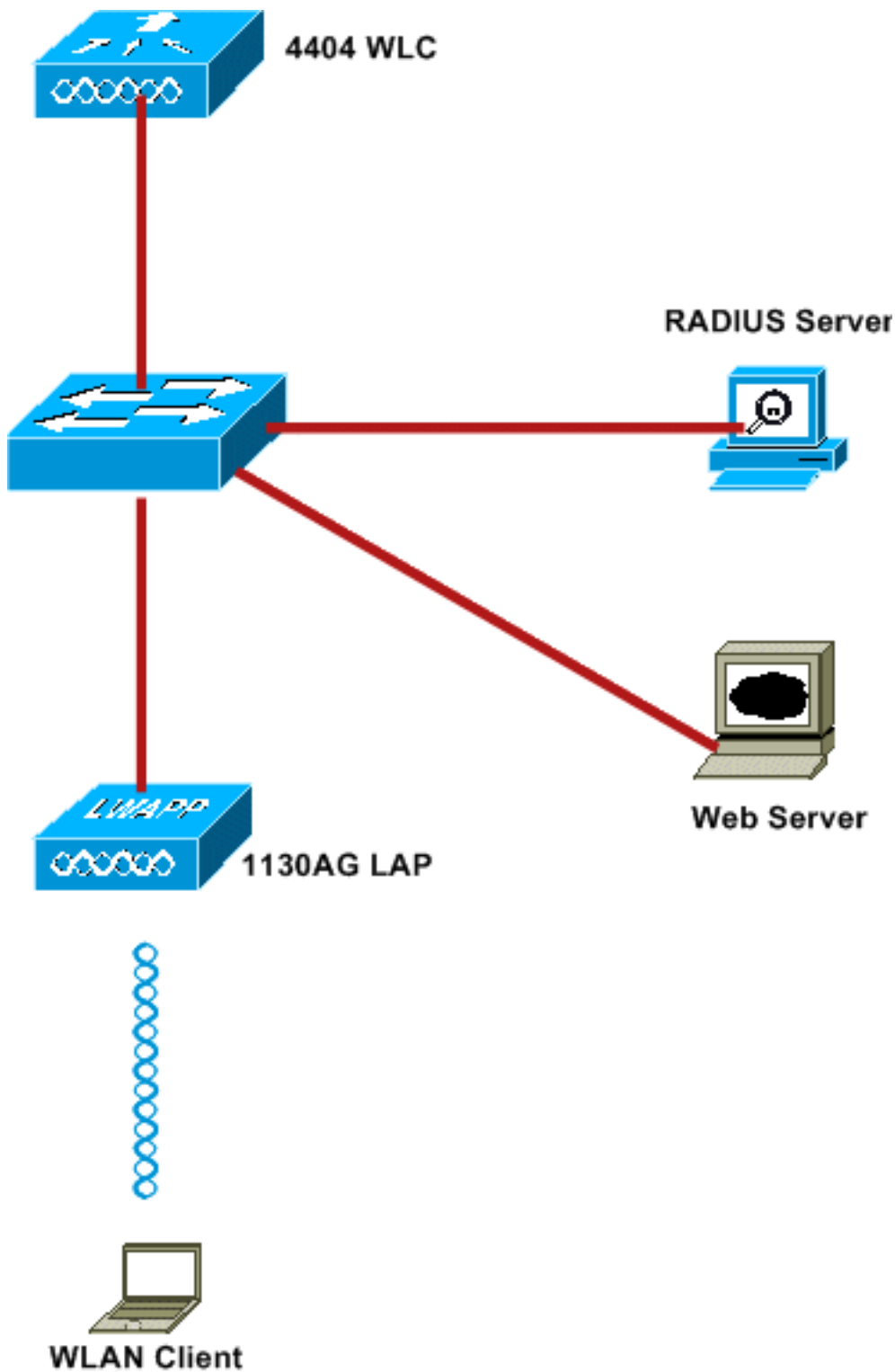
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Controller LAN wireless con firmware versione 5.0.148.0
- Cisco serie 1232 LAP
- Cisco 802.11a/b/g Wireless Client Adapter 3.6.0.61
- Server Web esterno che ospita la pagina di accesso per l'autenticazione Web
- Cisco Secure ACS versione con firmware 4.1.1.24

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.

## Esempio di rete

Nel documento viene usata questa impostazione di rete:



Di seguito vengono riportati gli indirizzi IP utilizzati nel presente documento:

- WLC utilizza l'indirizzo IP 10.77.244.206
- Il LAP è registrato sul WLC con indirizzo IP 10.77.244.199
- Il server Web utilizza l'indirizzo IP 10.77.244.210
- Il server Cisco ACS usa l'indirizzo IP 10.77.244.196
- Il client riceve un indirizzo IP dall'interfaccia di gestione mappata alla WLAN - 10.77.244.208

## Convenzioni

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

## Autenticazione Web esterna

L'autenticazione Web è un meccanismo di autenticazione di layer 3 utilizzato per autenticare gli utenti guest per l'accesso a Internet. Gli utenti autenticati tramite questo processo non saranno in grado di accedere a Internet fino a quando non completeranno il processo di autenticazione. Per informazioni complete sul processo di autenticazione Web esterno, vedere la sezione [Processo di autenticazione Web esterno](#) del documento [Esempio di configurazione dell'autenticazione Web esterna con i controller LAN wireless](#).

In questo documento viene illustrato un esempio di configurazione in cui l'autenticazione Web esterna viene eseguita utilizzando un server RADIUS esterno.

## Configurare il WLC

Nel presente documento, si presume che il WLC sia già configurato e che abbia un LAP registrato sul WLC. Nel documento si presume inoltre che il WLC sia configurato per il funzionamento di base e che i LAP siano registrati sul WLC. Se si è un nuovo utente che cerca di configurare il WLC per il funzionamento di base con i LAP, fare riferimento alla [registrazione di un Lightweight AP \(LAP\) su un Wireless LAN Controller \(WLC\)](#). Per visualizzare i LAP registrati sul WLC, selezionare **Wireless > All AP** (Tutti i LAP).

Dopo aver configurato il WLC per il funzionamento di base e avere uno o più LAP registrati per esso, è possibile configurare il WLC per l'autenticazione Web esterna utilizzando un server Web esterno. Nell'esempio, viene usato un Cisco Secure ACS versione 4.1.1.24 come server RADIUS. Innanzitutto, verrà configurato il WLC per questo server RADIUS e quindi verrà esaminata la configurazione richiesta sugli ACS protetti di Cisco per questa installazione.

## Configurazione del WLC per Cisco Secure ACS

Per aggiungere il server RADIUS sul WLC, effettuare i seguenti passaggi:

1. Dall'interfaccia utente del WLC, fare clic sul menu **SECURITY**.
2. Nel menu **AAA**, selezionare il sottomenu **Raggio > Autenticazione**.
3. Fare clic su **Nuovo** e immettere l'indirizzo IP del server RADIUS. Nell'esempio, l'indirizzo IP del server è *10.77.244.196*.
4. Immettere il segreto condiviso nel WLC. Il segreto condiviso deve essere configurato allo stesso modo sul WLC.
5. Per il formato segreto condiviso, scegliere **ASCII** o **Hex**. Lo stesso formato deve essere scelto sul WLC.
6. **1812** è il numero di porta utilizzato per l'autenticazione RADIUS.
7. Verificare che l'opzione Stato server sia impostata su **Abilitato**.
8. Selezionare la casella **Abilita** utente di rete per autenticare gli utenti di rete.
9. Fare clic su **Apply**  
(Applica).

The screenshot shows the Cisco WLC configuration interface for a new RADIUS Authentication Server. The left sidebar is under 'Security' with 'AAA' expanded to 'RADIUS'. The main area is titled 'RADIUS Authentication Servers > New' and contains the following fields:

- Server Index (Priority): 2
- Server IP Address: 10.77.244.196
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Key Wrap:  (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:  Enable
- Management:  Enable
- IPSec:  Enable

## [Configurazione della WLAN sul WLC per l'autenticazione Web](#)

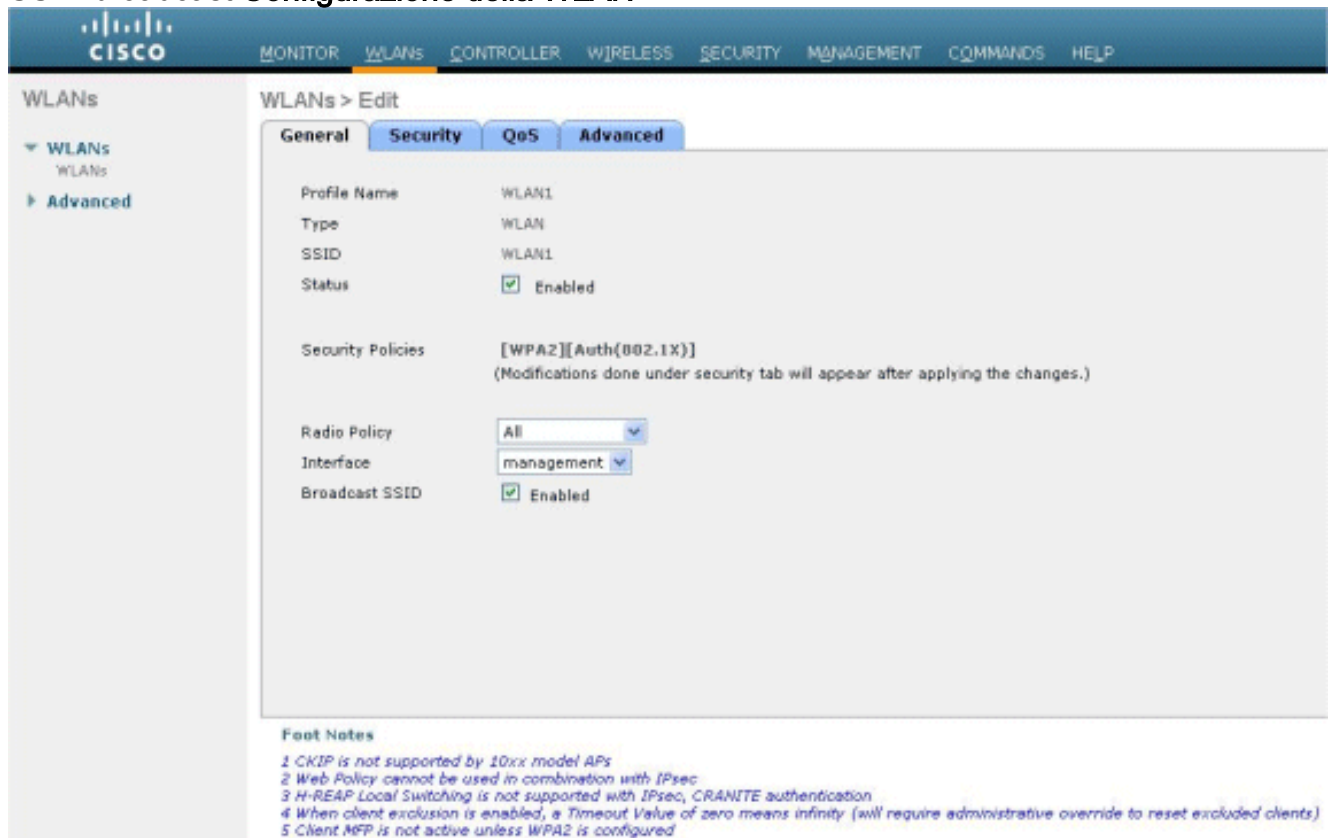
Il passaggio successivo è configurare la WLAN per l'autenticazione Web sul WLC. Per configurare la WLAN sul WLC, effettuare i seguenti passaggi:

1. Fare clic sul menu **WLAN** dall'interfaccia utente del controller e selezionare **New** (Nuovo).
2. Selezionate **WLAN** per Tipo (Type).
3. Immettere un nome di profilo e un SSID WLAN a scelta, quindi fare clic su **Apply** (Applica). **Nota:** per il SSID WLAN viene fatta distinzione tra maiuscole e minuscole.

The screenshot shows the Cisco WLC configuration interface for a new WLAN. The left sidebar is under 'WLANs' with 'Advanced' selected. The main area is titled 'WLANs > New' and contains the following fields:

- Type: WLAN
- Profile Name: WLAN1
- WLAN SSID: WLAN1

4. Nella scheda **Generale** verificare che l'opzione **Abilitato** sia selezionata sia per Stato che per SSID broadcast. **Configurazione della WLAN**



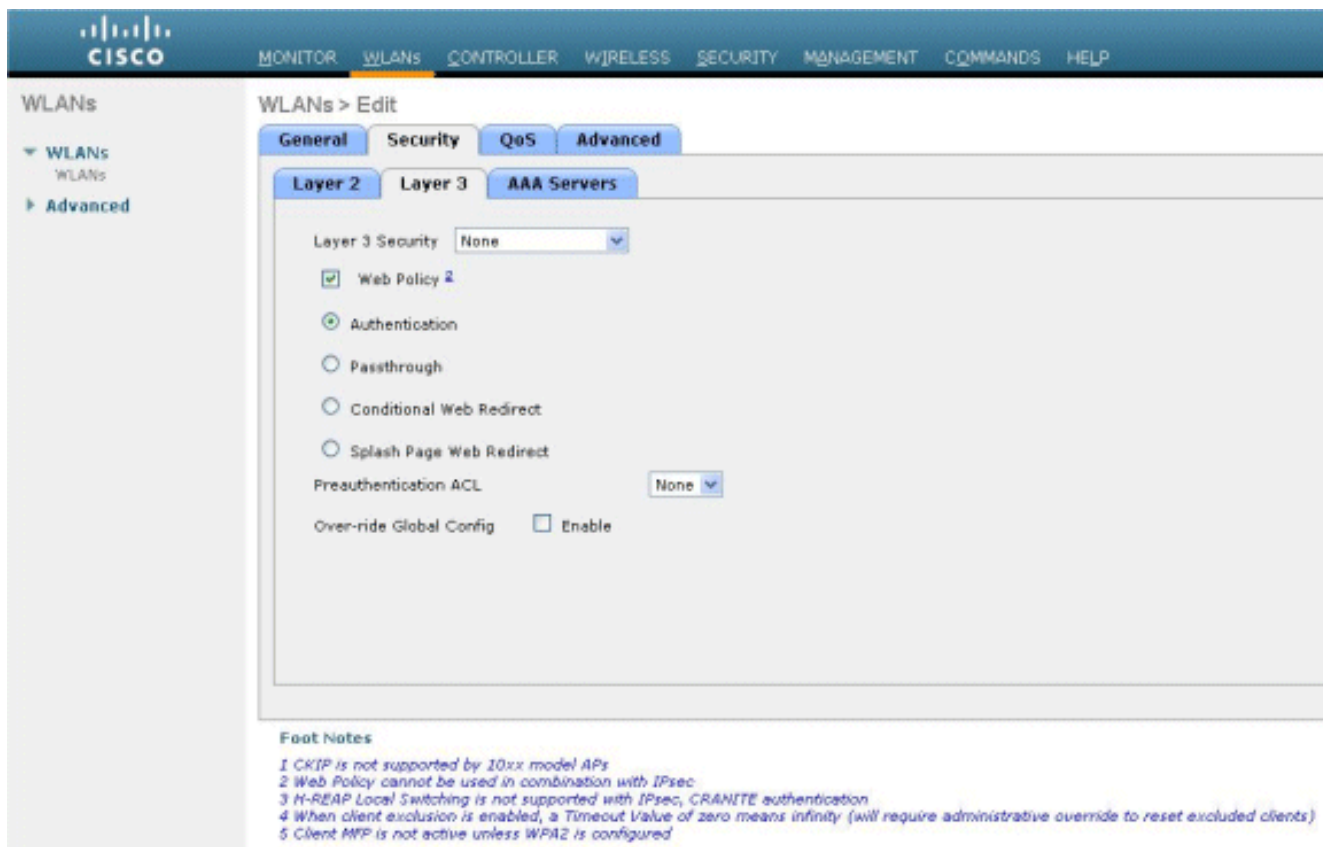
The screenshot shows the Cisco configuration interface for WLANs. The top navigation bar includes MONITOR, WLANs (selected), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows 'WLANs' with a sub-menu 'Advanced' selected. The main content area is titled 'WLANs > Edit' and has four tabs: General, Security, QoS, and Advanced. The 'General' tab is active, displaying the following configuration for 'WLAN1':

Profile Name	WLAN1
Type	WLAN
SSID	WLAN1
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface	management
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

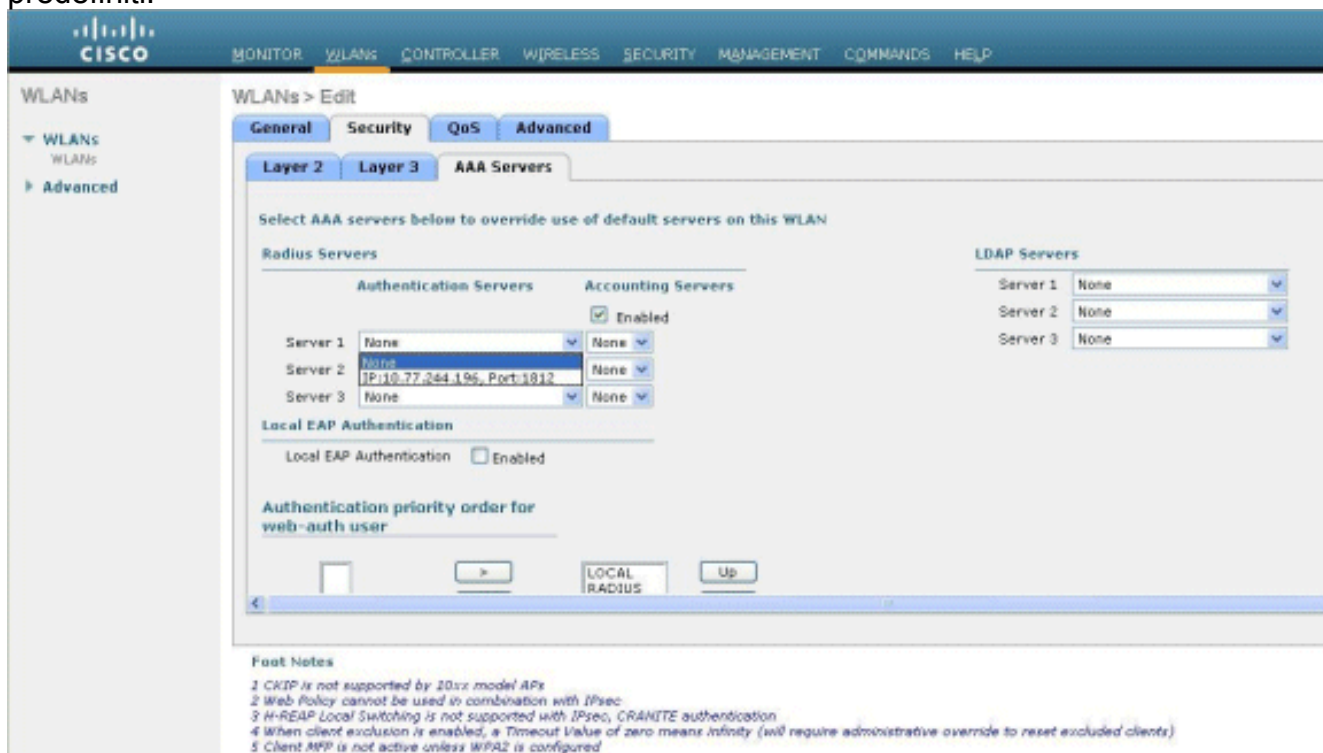
Below the configuration fields, there are 'Foot Notes':

- 1 CKIP 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

5. Selezionare un'interfaccia per la WLAN. In genere, un'interfaccia configurata in una VLAN univoca viene mappata alla WLAN in modo che il client riceva un indirizzo IP in tale VLAN. Nell'esempio, viene usata la *gestione* di Interface.
6. Scegliere la scheda **Protezione**.
7. Nel menu **Layer 2**, scegliere **Nessuno** per Protezione Layer 2.
8. Nel menu **Layer 3**, scegliere **Nessuno** per Protezione Layer 3. Selezionare la casella di controllo **Criterio Web** e scegliere **Autenticazione**.



9. Nel menu **Server AAA**, per Server di autenticazione, scegliere il server RADIUS configurato su questo WLC. Altri menu devono rimanere ai valori predefiniti.



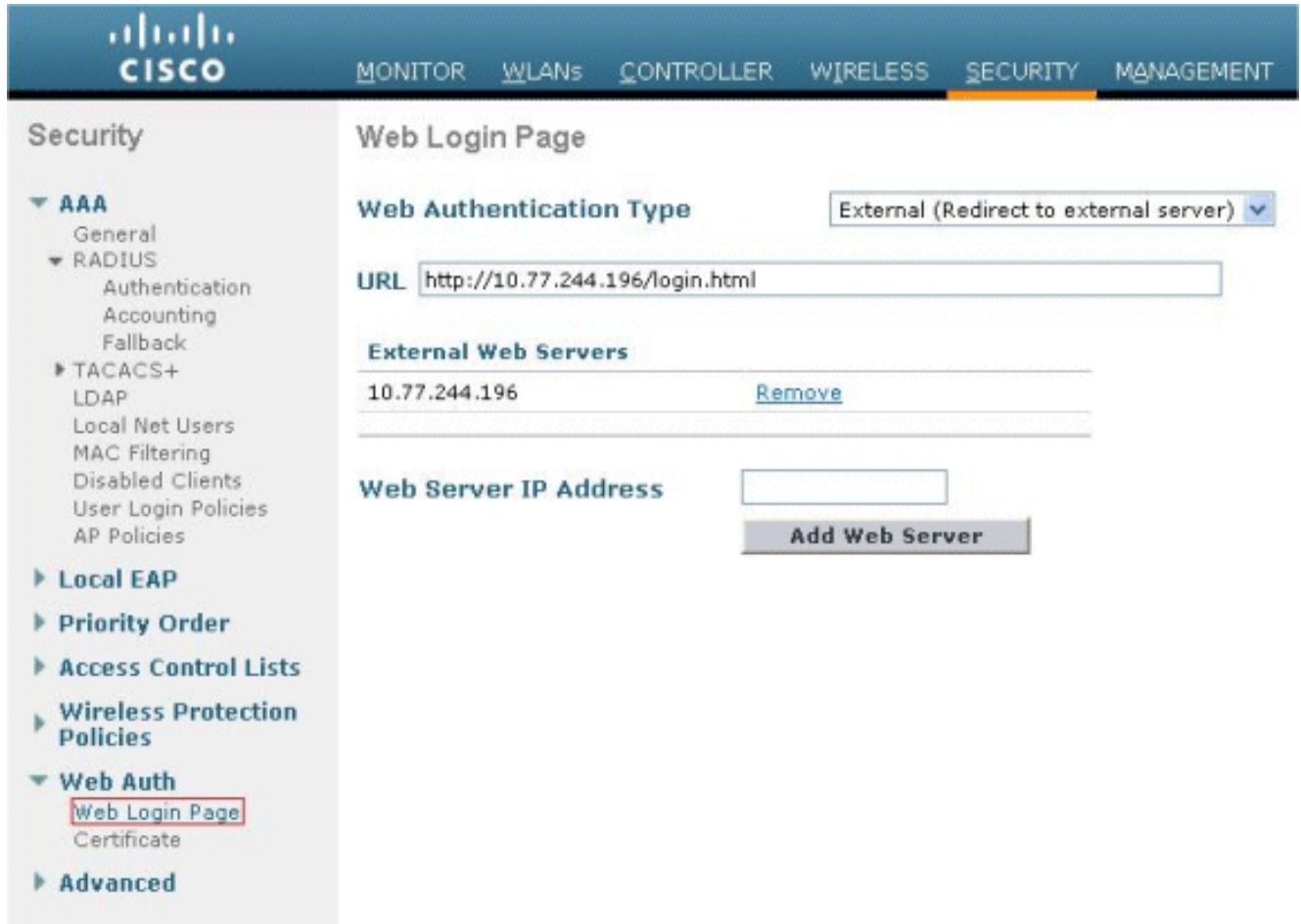
## [Configurare le informazioni sul server Web sul WLC](#)

Il server Web che ospita la pagina di autenticazione Web deve essere configurato sul WLC. Per configurare il server Web, attenersi alla procedura seguente:

1. Fare clic sulla scheda **Protezione**. Andare a **Web Auth > Pagina di login Web**.



2. Impostare il tipo di autenticazione Web su **Esterno**.
3. Nel campo Indirizzo IP server Web immettere l'indirizzo IP del server che ospita la pagina Autenticazione Web e fare clic su **Aggiungi server Web**. Nell'esempio, l'indirizzo IP è *10.77.244.196*, visualizzato in Server Web esterni.
4. Immettere l'URL per la pagina di autenticazione Web (in questo esempio, *http://10.77.244.196/login.html*) nel campo URL.



## [Configurazione di Cisco Secure ACS](#)

In questo documento si presume che Cisco Secure ACS Server sia già installato e in esecuzione su un computer. Per ulteriori informazioni su come configurare Cisco Secure ACS, consultare la [guida alla configurazione di Cisco Secure ACS 4.2](#).

## [Configurazione delle informazioni utente su Cisco Secure ACS](#)

Per configurare gli utenti su Cisco Secure ACS, eseguire la procedura seguente:

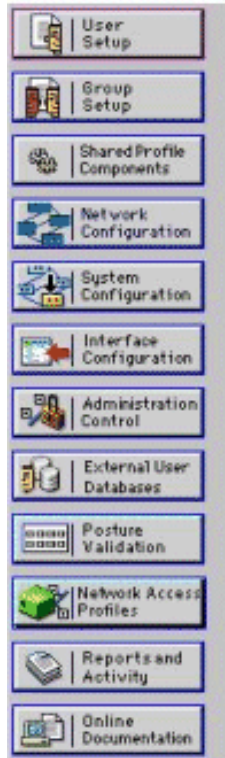
1. Selezionare **User Setup** (Configurazione utente) dall'interfaccia utente di Cisco Secure ACS, immettere un nome utente e fare clic su **Add/Edit** (Aggiungi/Modifica). In questo esempio, l'utente è *user1*.





## User Setup

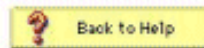
Select



User:

List users beginning with letter/number:

<a href="#">A</a>	<a href="#">B</a>	<a href="#">C</a>	<a href="#">D</a>	<a href="#">E</a>	<a href="#">F</a>	<a href="#">G</a>	<a href="#">H</a>	<a href="#">I</a>	<a href="#">J</a>	<a href="#">K</a>	<a href="#">L</a>	<a href="#">M</a>
<a href="#">N</a>	<a href="#">O</a>	<a href="#">P</a>	<a href="#">Q</a>	<a href="#">R</a>	<a href="#">S</a>	<a href="#">T</a>	<a href="#">U</a>	<a href="#">V</a>	<a href="#">W</a>	<a href="#">X</a>	<a href="#">Y</a>	<a href="#">Z</a>
<a href="#">0</a>	<a href="#">1</a>	<a href="#">2</a>	<a href="#">3</a>	<a href="#">4</a>	<a href="#">5</a>	<a href="#">6</a>	<a href="#">7</a>	<a href="#">8</a>	<a href="#">9</a>			



2. Per impostazione predefinita, il protocollo PAP viene utilizzato per autenticare i client. La password dell'utente viene immessa in **Configurazione utente > Autenticazione password > Cisco Secure PAP**. Accertarsi di scegliere **Database interno ACS** per Autenticazione password.

The screenshot shows the Cisco User Setup interface. On the left is a navigation menu with options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main area is titled 'User Setup' and contains the following fields and options:

- Account Disabled
- Supplementary User Info** (with a help icon):
  - Real Name:
  - Description:
- User Setup** (with a help icon):
  - Password Authentication:  (dropdown menu)
  - CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)
  - Password:
  - Confirm Password:
  - Separate (CHAP/MS-CHAP/ARAP)
    - Password:
    - Confirm Password:
  - When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.
  - Group to which the user is assigned:  (dropdown menu)

At the bottom are 'Submit' and 'Cancel' buttons.

3. All'utente deve essere assegnato un gruppo a cui appartiene. Scegliere il **gruppo predefinito**.
4. Fare clic su **Invia**.

## [Configurazione delle informazioni WLC su Cisco Secure ACS](#)

Eseguire questi passaggi per configurare le informazioni WLC su Cisco Secure ACS:

1. Nell'interfaccia utente di ACS, fare clic sulla scheda **Network Configuration** (Configurazione di rete), quindi su **Add Entry** (Aggiungi voce).
2. Viene visualizzata la schermata Add AAA client (Aggiungi client AAA).
3. Immettere il nome del client. Nell'esempio, viene utilizzato *WLC*.
4. Immettere l'indirizzo IP del client. L'indirizzo IP del WLC è *10.77.244.206*.
5. Immettere la chiave segreta condivisa e il formato della chiave. Questa opzione dovrebbe corrispondere alla voce creata nel menu **Security** del WLC.
6. Scegliere **ASCII** per il formato di input della chiave, che deve essere lo stesso sul WLC.
7. Per impostare il protocollo utilizzato tra il WLC e il server RADIUS, selezionare **RADIUS (Cisco Airespace)** per Authenticate Using.
8. Fare clic su **Submit + Apply (Invia +**

Applica).

**Network Configuration**

**Add AAA Client**

AAA Client Hostname: WLC

AAA Client IP Address: 10.77.244.206

Shared Secret: abc123

**RADIUS Key Wrap**

Key Encryption Key: [ ]

Message Authenticator Code Key: [ ]

Key Input Format:  ASCII  Hexadecimal

Authenticate Using: RADIUS (Cisco Airespace)

Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

Submit Submit + Apply Cancel

Back to Help

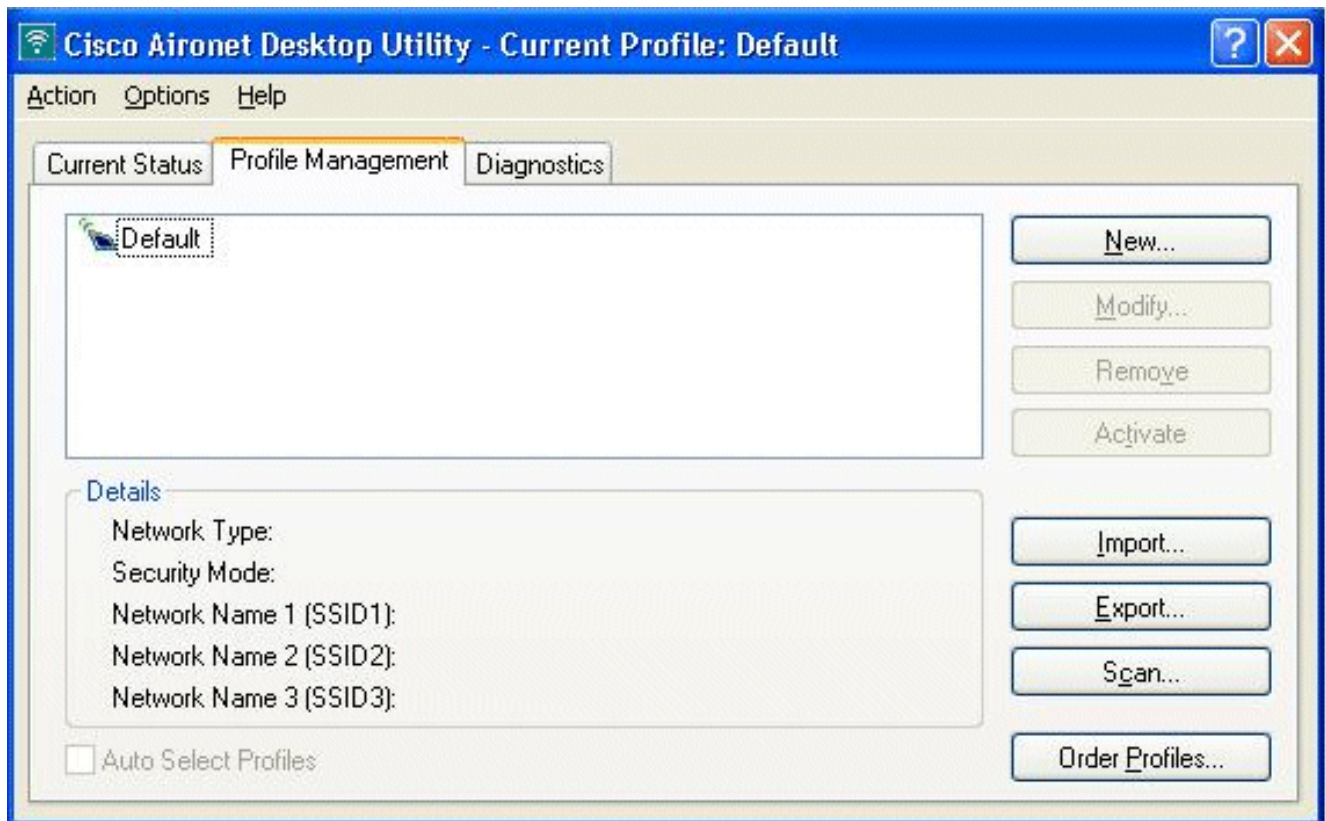
## Processo di autenticazione client

### Configurazione client

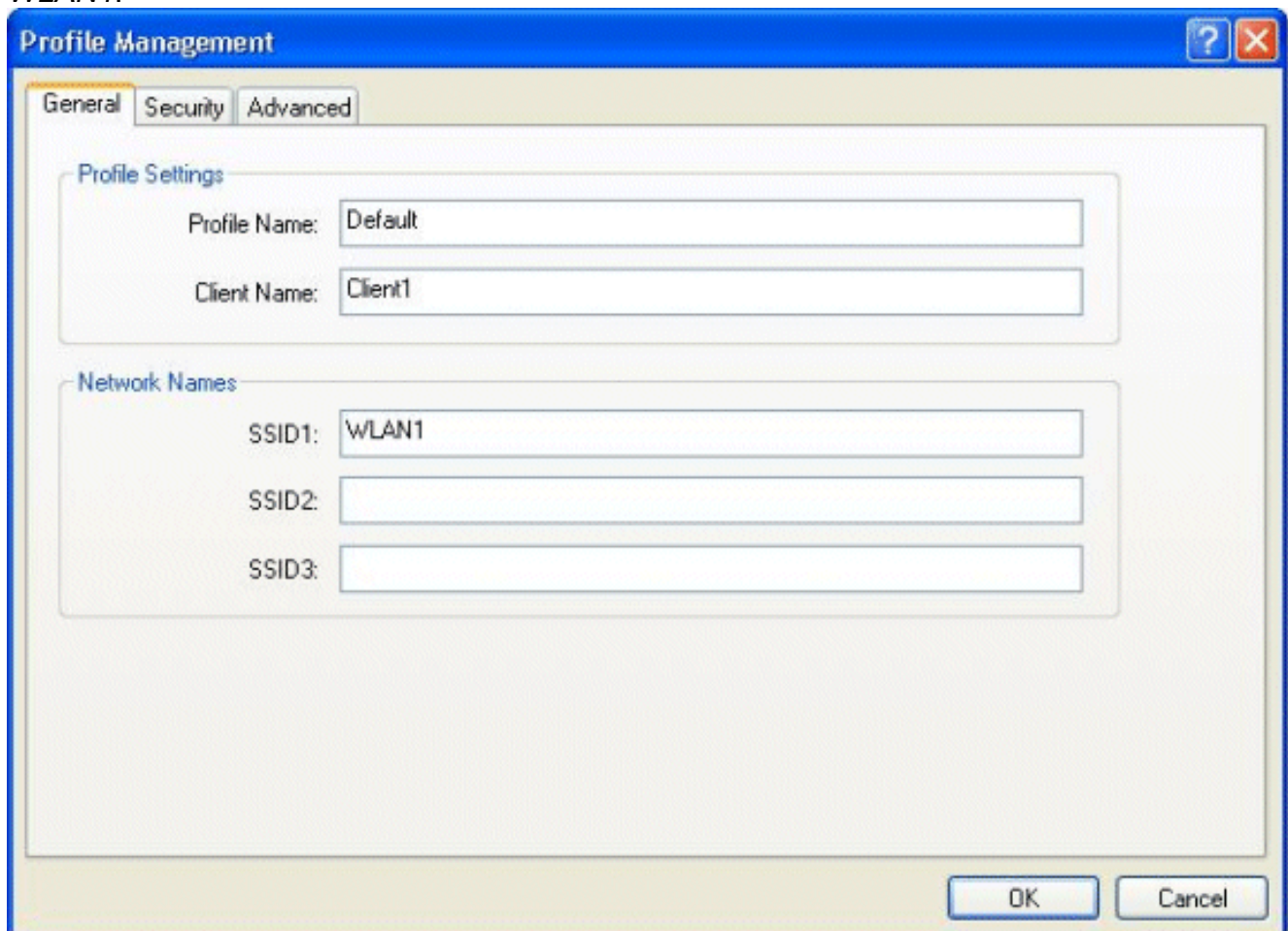
Nell'esempio, viene usata Cisco Aironet Desktop Utility per eseguire l'autenticazione Web. Eseguire questa procedura per configurare Aironet Desktop Utility.

1. Aprire Aironet Desktop Utility da **Start > Cisco Aironet > Aironet Desktop Utility**.
2. Fare clic sulla scheda **Gestione profili**.



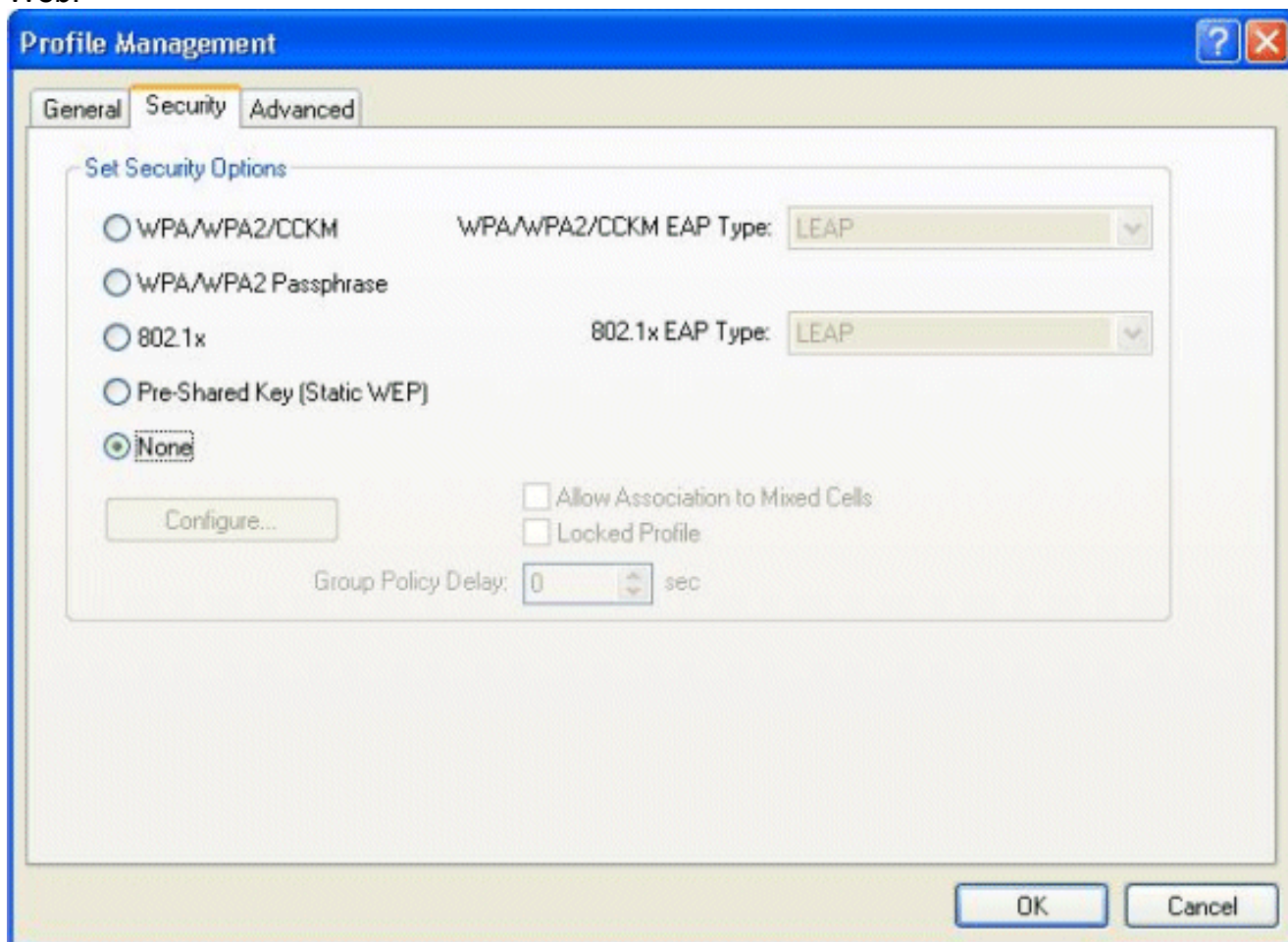


3. Scegliere il profilo **predefinito** e fare clic su **Modifica**. Fare clic sulla scheda **Generale**. Configurare il nome di un profilo. Nell'esempio viene utilizzato *Default*. Configurare il SSID in Nomi di rete, nell'esempio viene usata *WLAN1*.



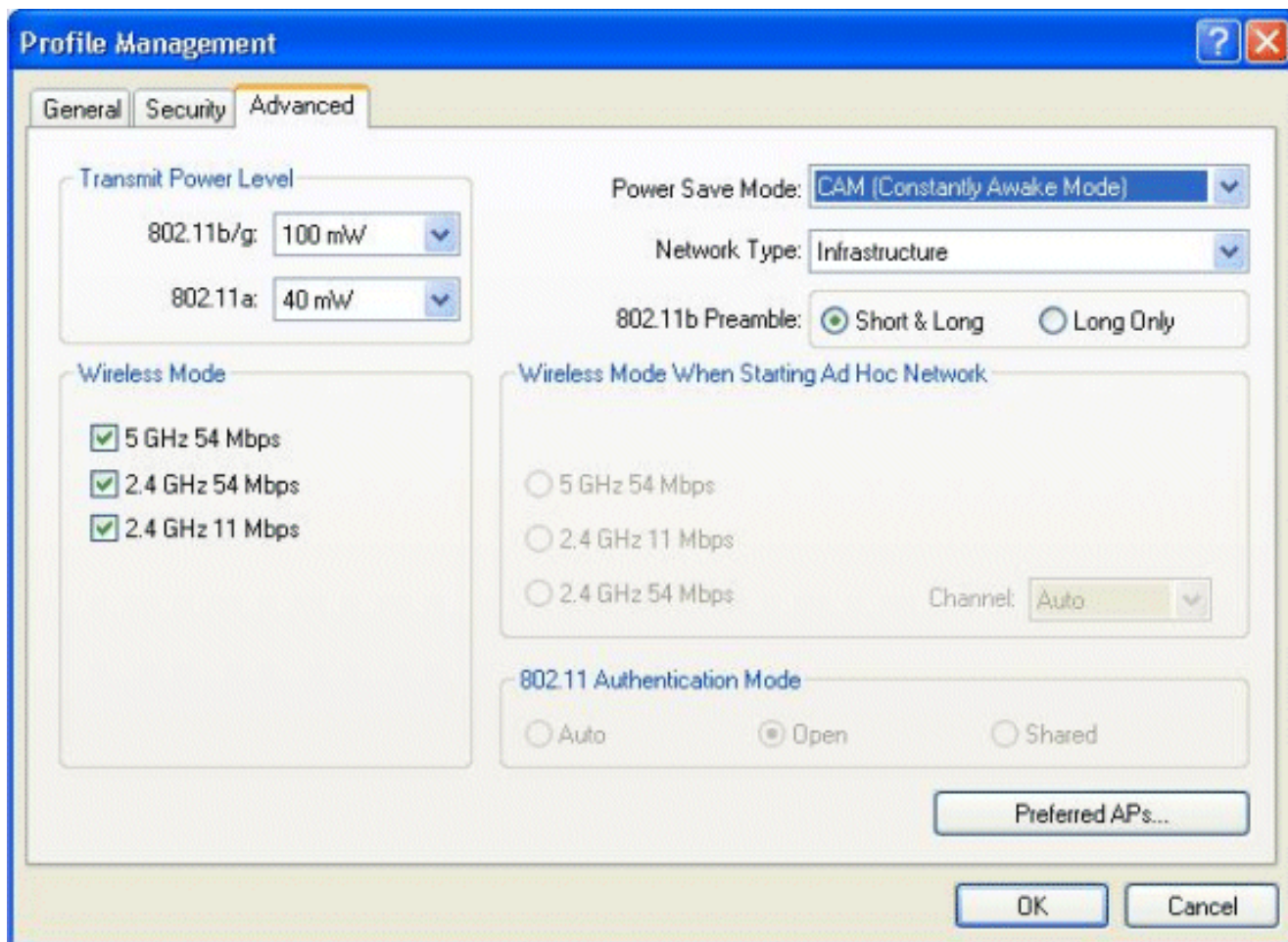
**Nota:** l'SSID fa distinzione tra maiuscole e minuscole e deve corrispondere alla WLAN configurata sul WLC. Fare clic sulla scheda **Protezione**. Scegliete **Nessuno** come Protezione

per l'autenticazione Web.



Fare clic sulla scheda **Avanzate**. Nel menu **Modalità wireless**, scegliere la frequenza con cui il client wireless comunica con il LAP. In **Livello potenza di trasmissione**, scegliere la potenza configurata sul WLC. Accettare il valore predefinito per Modalità risparmio energia. Nel campo Network Type (Tipo di rete), selezionare **Infrastructure** (Infrastruttura). Impostare il preambolo 802.11b come **breve e lungo** per una migliore compatibilità. Fare clic su **OK**.



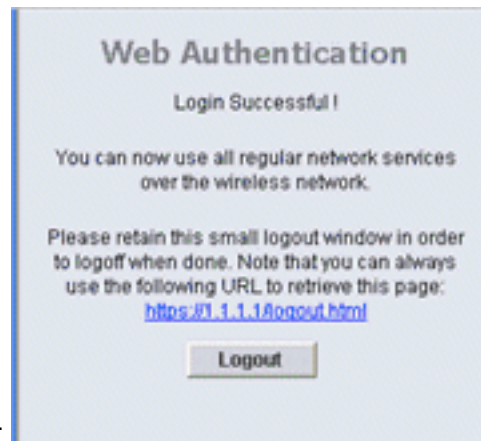


4. Dopo aver configurato il profilo sul software del client, il client viene associato correttamente e riceve un indirizzo IP dal pool di VLAN configurato per l'interfaccia di gestione.

## Processo di login client

Questa sezione spiega come avviene l'accesso client.

1. Aprire una finestra del browser e immettere un URL o un indirizzo IP. In questo modo la pagina di autenticazione Web viene visualizzata sul client. Se sul controller è in esecuzione una release precedente alla 3.0, l'utente deve immettere `https://1.1.1.1/login.html` per visualizzare la pagina di autenticazione Web. Viene visualizzata una finestra di avviso di protezione.
2. Per continuare, fare clic su **Yes** (Sì).
3. Quando viene visualizzata la finestra Accesso, immettere il nome utente e la password configurati sul server RADIUS. Se l'accesso ha esito positivo, verranno visualizzate due finestre del browser. La finestra ingrandita indica che l'accesso è riuscito ed è possibile accedere a questa finestra per navigare su Internet. Utilizzare la finestra più piccola per



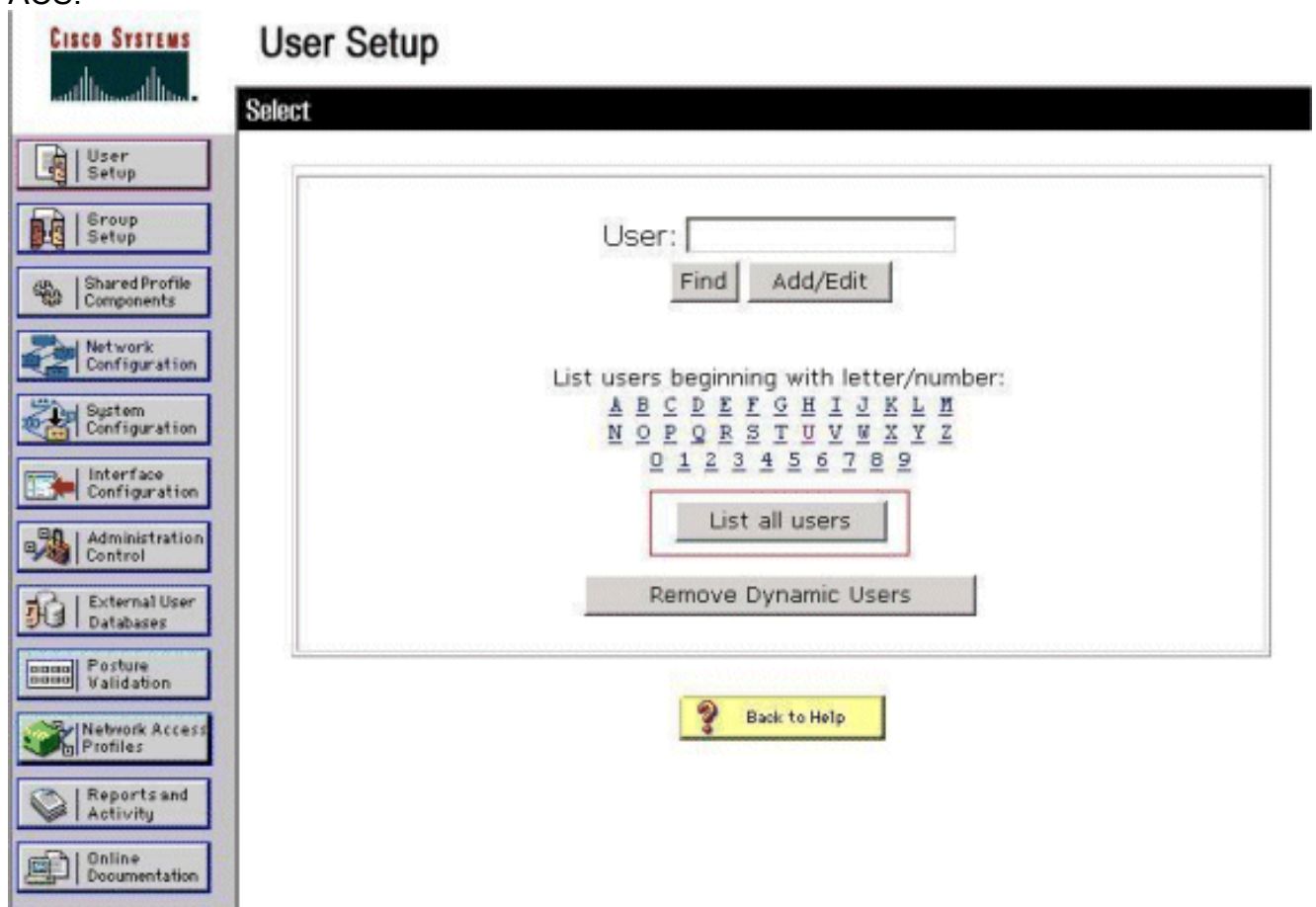
disconnettersi al termine dell'utilizzo della rete guest.

## Verifica

Per un'autenticazione Web corretta, è necessario verificare che i dispositivi siano configurati correttamente. Questa sezione spiega come verificare i dispositivi usati nel processo.

## Verifica ACS

1. Fare clic su **User Setup** (Configurazione utente), quindi su **List All Users** (Elenca tutti gli utenti) nell'interfaccia utente di ACS.



Verificare che lo stato dell'utente sia *Abilitato* e che il gruppo Predefinito sia mappato all'utente.



## User List

User	Status	Group	Network Access Profile
<a href="#">user1</a>	Enabled	Default Group (2 users)	(Default)

2. Fare clic sulla scheda **Network Configuration** (Configurazione di rete) e cercare nella tabella **AAA Client** per verificare che il WLC sia configurato come client AAA.

The screenshot shows the Cisco Network Configuration interface. On the left is a navigation menu with options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Profile Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled "Network Configuration" and contains three tables:

- AAA Clients:** A table with columns "AAA Client Hostname", "AAA Client IP Address", and "Authenticate Using". It contains one entry: [wlc1](#), 10.77.244.206, RADIUS (Cisco Airespace). Buttons: "Add Entry", "Search".
- AAA Servers:** A table with columns "AAA Server Name", "AAA Server IP Address", and "AAA Server Type". It contains one entry: [TS-Web](#), 10.77.244.196, CiscoSecure ACS. Buttons: "Add Entry", "Search".
- Proxy Distribution Table:** A table with columns "Character String", "AAA Servers", "Strip", and "Account". It contains one entry: [\(Default\)](#), TS-Web, No, Local. Buttons: "Add Entry", "Sort Entries".

At the bottom of the main content area is a "Back to Help" button.

## Verifica WLC

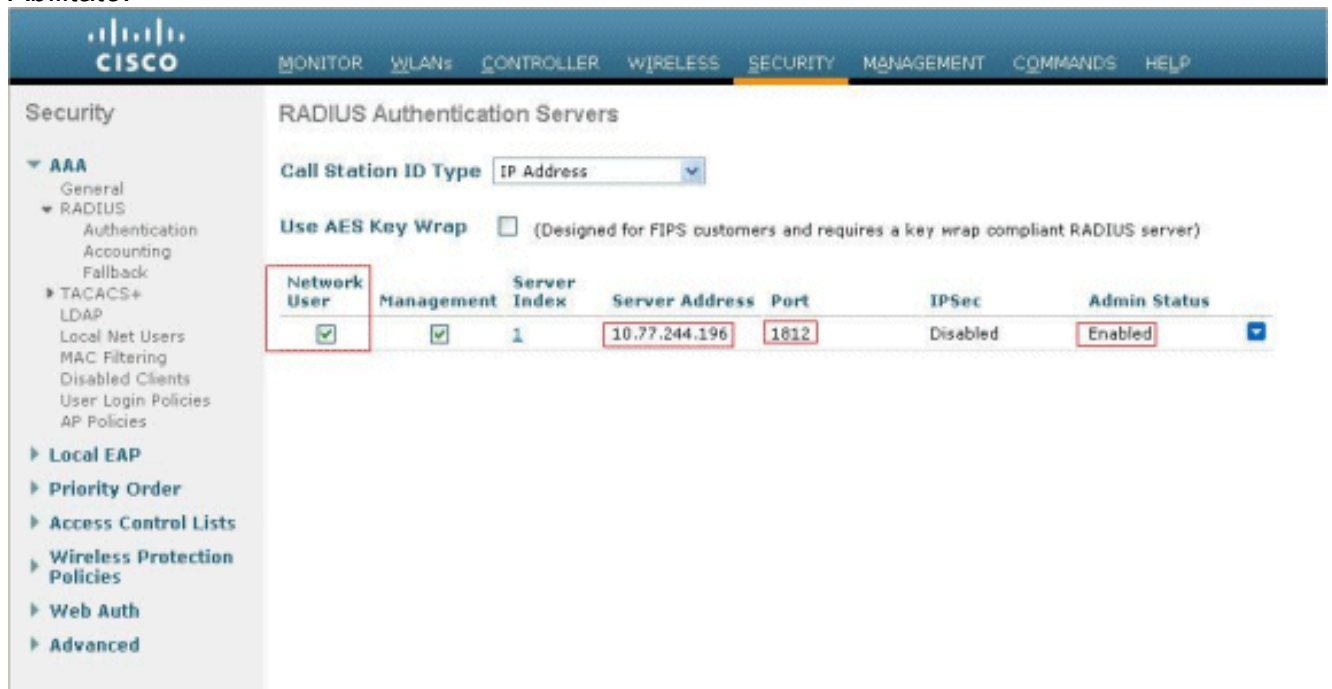
1. Fare clic sul menu **WLAN** dall'interfaccia utente del WLC. Verificare che la WLAN utilizzata per l'autenticazione Web sia elencata nella pagina. Verificare che lo stato di amministrazione della WLAN sia *Abilitato*. Verificare che nei Criteri di sicurezza per la WLAN sia indicato *Web-Auth*.

The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes "MONITOR", "WLANs", "CONTROLLER", "WIRELESS", "SECURITY", "MANAGEMENT", "COMMANDS", and "HELP". The "WLANs" menu is expanded, showing "WLANs" and "Advanced". The main content area is titled "WLANs" and contains a table:

Profile Name	Type	WLAN SSID	Admin Status	Security Policies
<a href="#">WLAN1</a>	WLAN	<a href="#">WLAN1</a>	<a href="#">Enabled</a>	<a href="#">Web-Auth</a>

2. Fare clic sul menu **SECURITY** (SICUREZZA) dall'interfaccia utente del WLC. Verificare che

Cisco Secure ACS (10.77.244.196) sia elencato nella pagina. Assicurarsi che la casella Utente di rete sia selezionata. Verificare che la porta sia 1812 e che lo stato dell'amministratore sia *Abilitato*.



## Risoluzione dei problemi

L'autenticazione Web non è riuscita per diversi motivi. Il documento [Troubleshooting Web Authentication on a Wireless LAN Controller \(WLC\)](#) spiega chiaramente questi motivi in dettaglio.

## Comandi per la risoluzione dei problemi

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

Telnet nel WLC e usare questi comandi per risolvere i problemi di autenticazione:

- **debug aaa all enable**

```

Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Successful transmission of Authentic
ation Packet (id 1) to 10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:01
Fri Sep 24 13:59:52 2010: 00000000: 01 01 00 73 00 00 00 00 00 00 00 00 00 0
0 00 ...s.....
Fri Sep 24 13:59:52 2010: 00000010: 00 00 00 00 01 07 75 73 65 72 31 02 12 93 c
3 66 .....user1....f
Fri Sep 24 13:59:52 2010: 00000030: 75 73 65 72 31
user1
Fri Sep 24 13:59:52 2010: ****Enter processIncomingMessages: response code=2
Fri Sep 24 13:59:52 2010: ****Enter processRadiusResponse: response code=2
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Access-Accept received from RADIUS s
erver 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 0
Fri Sep 24 13:59:52 2010: AuthorizationResponse: 0x12238db0
Fri Sep 24 13:59:52 2010: structureSize.....89
Fri Sep 24 13:59:52 2010: resultCode.....0
Fri Sep 24 13:59:52 2010: protocolUsed.....0x0
0000001
Fri Sep 24 13:59:52 2010: proxyState.....00:

```

```

40:96:AC:DD:05-00:00
Fri Sep 24 13:59:52 2010:      Packet contains 2 AVPs:
Fri Sep 24 13:59:52 2010:      AVP[01] Framed-IP-Address.....
.....0xffffffff (-1) (4 bytes)
Fri Sep 24 13:59:52 2010:      AVP[02] Class.....
.....CACs:0/5183/a4df4ce/user1 (25 bytes)
Fri Sep 24 13:59:52 2010: Authentication failed for user1, Service Type: 0
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Applying new AAA override for station
00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Override values for station 00:40:96
:ac:dd:05
                source: 48, valid bits: 0x1
                qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

dataAvgC: -1, rTavgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                vlanIfName: '',
aclName:
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Unable to apply override policy for
station 00:40:96:ac:dd:05 - VapAllowRadiusOverride is FALSE
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Sending Accounting request (0) for s
tation 00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: AccountingMessage Accounting Start: 0x1500501c
Fri Sep 24 13:59:52 2010:      Packet contains 12 AVPs:
Fri Sep 24 13:59:52 2010:      AVP[01] User-Name.....
.....user1 (5 bytes)
Fri Sep 24 13:59:52 2010:      AVP[02] Nas-Port.....
.....0x00000002 (2) (4 bytes)
Fri Sep 24 13:59:52 2010:      AVP[03] Nas-Ip-Address.....
.....0x0a4df4ce (172881102) (4 bytes)
Fri Sep 24 13:59:52 2010:      AVP[04] Framed-IP-Address.....
.....0x0a4df4c7 (172881095) (4 bytes)

```

- **abilitazione dettagli debug aaa**

I tentativi di autenticazione non riusciti sono elencati nel menu disponibile in **Report e attività > Tentativi non riusciti**.

## [Informazioni correlate](#)

- [Esempio di configurazione dell'autenticazione Web del controller LAN wireless](#)
- [Risoluzione dei problemi di autenticazione Web su un controller WLC](#)
- [Esempio di configurazione dell'autenticazione Web esterna con i controller LAN wireless](#)
- [Esempio di configurazione dell'autenticazione Web con LDAP sui Wireless LAN Controller \(WLC\)](#)
- [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).