Esempio di configurazione di ACL per utente con controller LAN wireless e Cisco Secure ACS

Sommario

Introduzione

In questo documento viene spiegato come creare elenchi di controllo di accesso (ACL) sui WLC e applicarli agli utenti che dipendono dall'autorizzazione RADIUS.

Prerequisiti

Requisiti

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

- Conoscenze base di come configurare un server Cisco Secure ACS per autenticare i client wireless
- Conoscenza della configurazione dei Cisco Aironet Lightweight Access Point (LAP) e dei Cisco Wireless LAN Controller (WLC)

- Conoscenza delle soluzioni Cisco Unified Wireless Security

Componenti usati

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

- Cisco serie 4400 Wireless LAN Controller con versione 5.0.148.0
- Cisco Aironet serie 1231 Lightweight Access Point (LAP)
- Cisco Aironet 802.11 a/b/g Adattatore client LAN wireless Cisco con versione 3.6
- Cisco Aironet Desktop Utility versione 3.6
- Cisco Secure ACS Server versione 4.1
- Cisco serie 2800 Integrated Services Router con IOS® versione 12.4(11)T
- Cisco Catalyst serie 2900XL Switch con versione 12.0(5)WC3b

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.

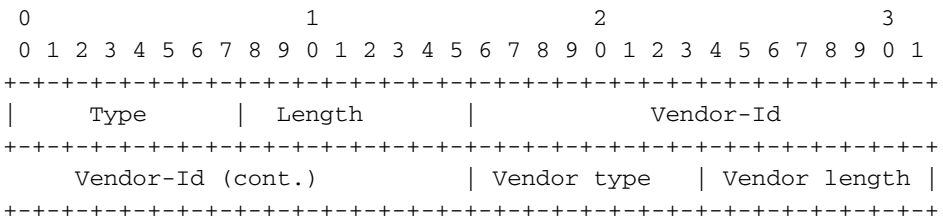
Premesse

L'elenco di controllo di accesso (ACL) per utente fa parte di Cisco Identity networking. Cisco Wireless LAN Solution supporta le reti di identità che, oltre a consentire alla rete di annunciare un singolo SSID, consentono anche a utenti specifici di ereditare policy diverse in base al proprio profilo utente.

La funzionalità ACL per utente consente di applicare a un utente un ACL configurato sul controller LAN wireless in base all'autorizzazione RADIUS. A tale scopo, usare l'attributo specifico del fornitore Airespace-ACL-Name (VSA).

Questo attributo indica il nome ACL da applicare al client. Quando l'attributo ACL è presente in Accetta accesso RADIUS, il sistema applica il nome ACL alla stazione client dopo l'autenticazione. In questo modo si ignorano gli ACL assegnati all'interfaccia. Ignora l'ACL di interfaccia assegnato e applica quello nuovo.

Di seguito è riportato un riepilogo del formato dell'attributo ACL-Name. I campi vengono trasmessi da sinistra a destra



```
|        ACL Name...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

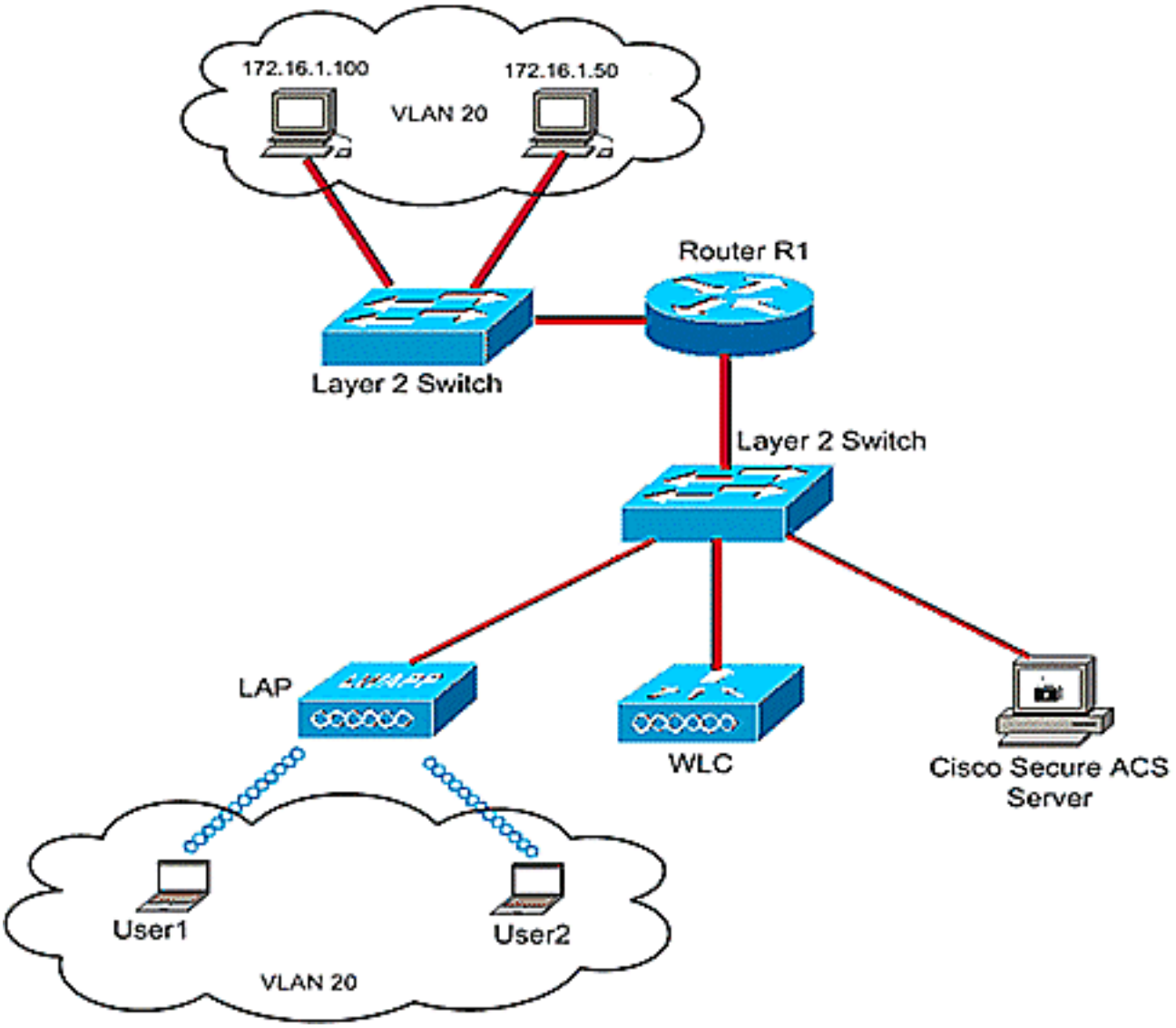
- Type - 26 for Vendor-Specific
- Length - >7
- Vendor-Id - 14179
- Vendor type - 6
- Vendor length - >0
- Value - A string that includes the name of the ACL to use for the client.
  The string is case sensitive.

Per ulteriori informazioni su Cisco Unified Wireless Network Identity Networking, fare riferimento alla sezione Configurazione di Identity Networking del documento Configurazione di soluzioni di sicurezza.

Esempio di rete

Nel documento viene usata questa impostazione di rete:

In questa configurazione, i controller WLC e LAP della LAN wireless vengono usati per fornire servizi wireless agli utenti del Reparto A e del Reparto B. Tutti gli utenti wireless utilizzano un ufficio WLAN (SSID) comune per accedere alla rete e si trovano nella VLAN Office-VLAN.



Il server Cisco Secure ACS viene utilizzato per autenticare gli utenti wireless. L'autenticazione EAP viene utilizzata per autenticare gli utenti. Il WLC, il LAP e il server Cisco Secure ACS sono

collegati a uno switch di layer 2, come mostrato.

Il router R1 connette i server sul lato cablato tramite lo switch di layer 2, come mostrato. Il router R1 funge anche da server DHCP, che fornisce indirizzi IP ai client wireless dalla subnet 172.16.0.0/16.

Ènecessario configurare i dispositivi in modo che si verifichi quanto segue:

L'utente 1 del reparto A ha accesso solo al server 172.16.1.100

L'utente 2 del reparto B ha accesso solo al server 172.16.1.50

A tale scopo, è necessario creare 2 ACL sul WLC: uno per l'utente 1 e l'altro per l'utente 2. Dopo aver creato gli ACL, è necessario configurare il server Cisco Secure ACS in modo che restituisca l'attributo del nome ACL al WLC una volta completata l'autenticazione dell'utente wireless. Il WLC applica quindi l'ACL all'utente, e quindi la rete è soggetta a restrizioni a seconda del profilo utente.

Nota: questo documento utilizza l'autenticazione LEAP per autenticare gli utenti. Cisco LEAP è vulnerabile agli attacchi dei dizionari. Nelle reti in tempo reale è consigliabile utilizzare metodi di autenticazione più sicuri, ad esempio EAP FAST. Poiché lo scopo del documento è spiegare come configurare la funzione ACL Per Utente, LEAP viene usato per semplicità.

Nella sezione successiva vengono fornite istruzioni dettagliate per la configurazione delle periferiche per questa installazione.

Configurazione

Prima di configurare la funzionalità degli ACL per utente, è necessario configurare il WLC per il funzionamento di base e registrare i LAP sul WLC. In questo documento si presume che il WLC sia configurato per il funzionamento di base e che i LAP siano registrati sul WLC. Se si è un nuovo utente e si 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).

Una volta registrati i LAP, attenersi alla seguente procedura per configurare i dispositivi per questa configurazione:

1. Configurare il controller LAN wireless.
2. Configurare il server Cisco Secure ACS.
3. Verificare la configurazione.

Nota: in questo documento viene descritta la configurazione richiesta sul lato wireless. Nel documento si presume che la configurazione cablata sia attiva.

Configurazione del controller LAN wireless

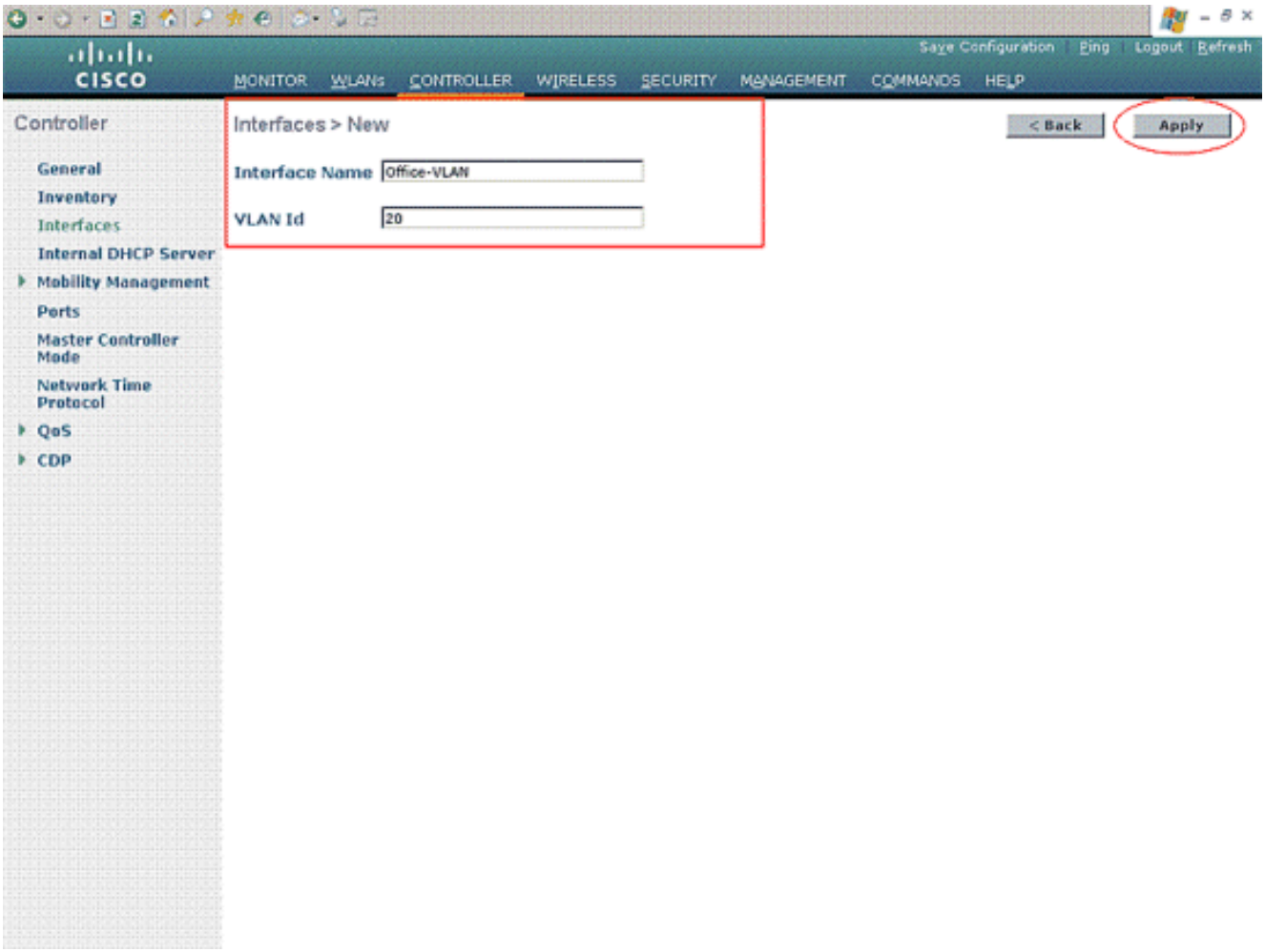
Sul controller LAN wireless, procedere come segue:

- Creare una VLAN per gli utenti wireless.
- Configurare il WLC per autenticare gli utenti wireless con Cisco Secure ACS.
- Crea una nuova WLAN per gli utenti wireless.
- Definire gli ACL per gli utenti wireless.

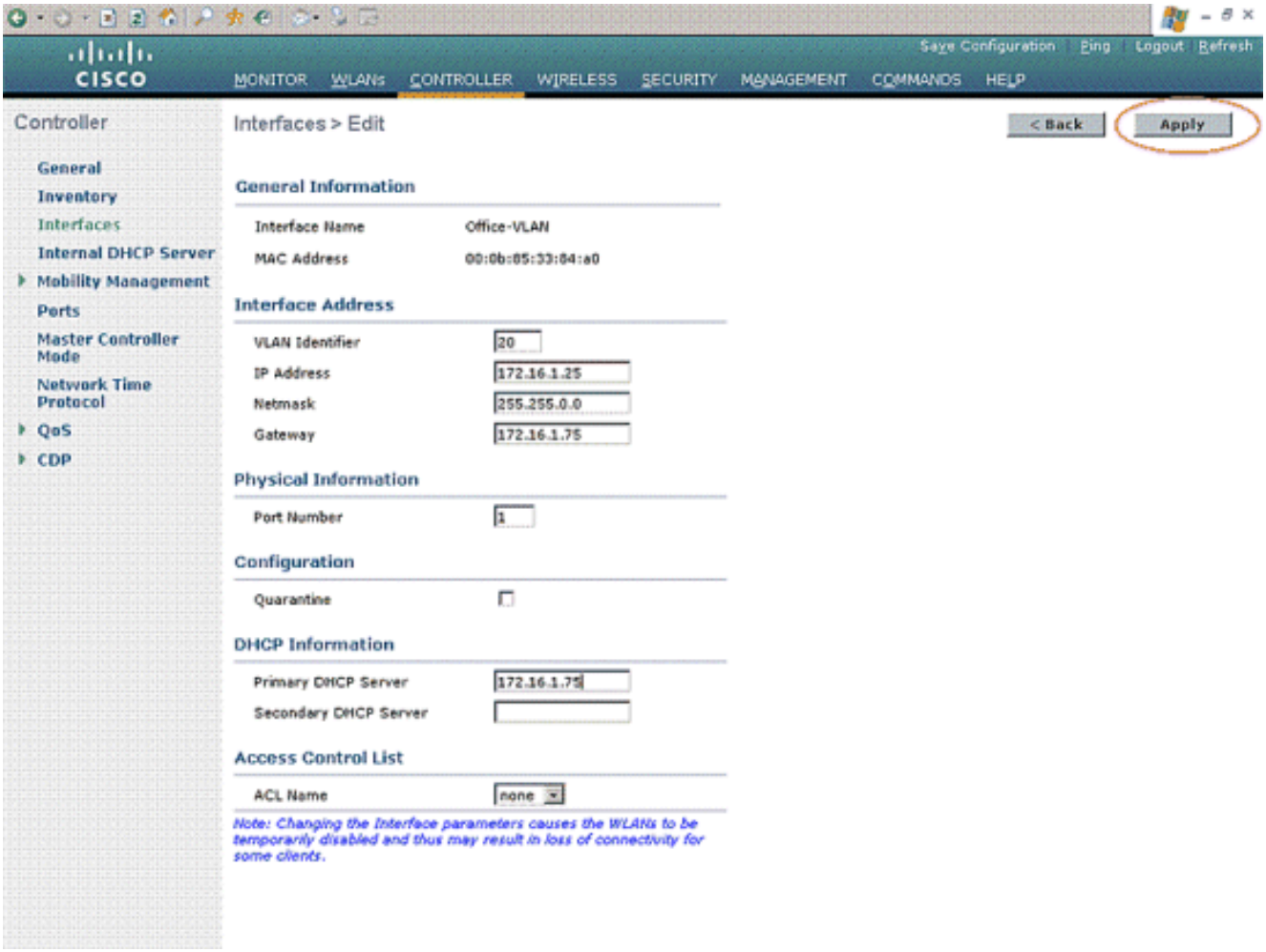
Creazione di una VLAN per gli utenti wireless

Per creare una VLAN per gli utenti wireless, attenersi alla seguente procedura.

1. Andare alla GUI del WLC e scegliere **Controller > Interfacce**. Viene visualizzata la finestra Interfacce. In questa finestra sono elencate le interfacce configurate sul controller.
2. Per creare una nuova interfaccia dinamica, fare clic su **New** (Nuovo).
3. Nella finestra **Interfacce > Nuovo**, immettere il nome dell'interfaccia e l'ID VLAN. Quindi fare clic su Applica. Nell'esempio, il nome dell'interfaccia dinamica è Office-VLAN e l'ID della VLAN è
   20.



4. Nella finestra **Interfacce > Modifica**, immettere l'indirizzo IP, la subnet mask e il gateway predefinito per l'interfaccia dinamica. Assegnarla a una porta fisica sul WLC e immettere l'indirizzo IP del server DHCP. Quindi fare clic su
   Applica.



Nell'esempio, questi parametri sono usati per l'interfaccia Office-VLAN:

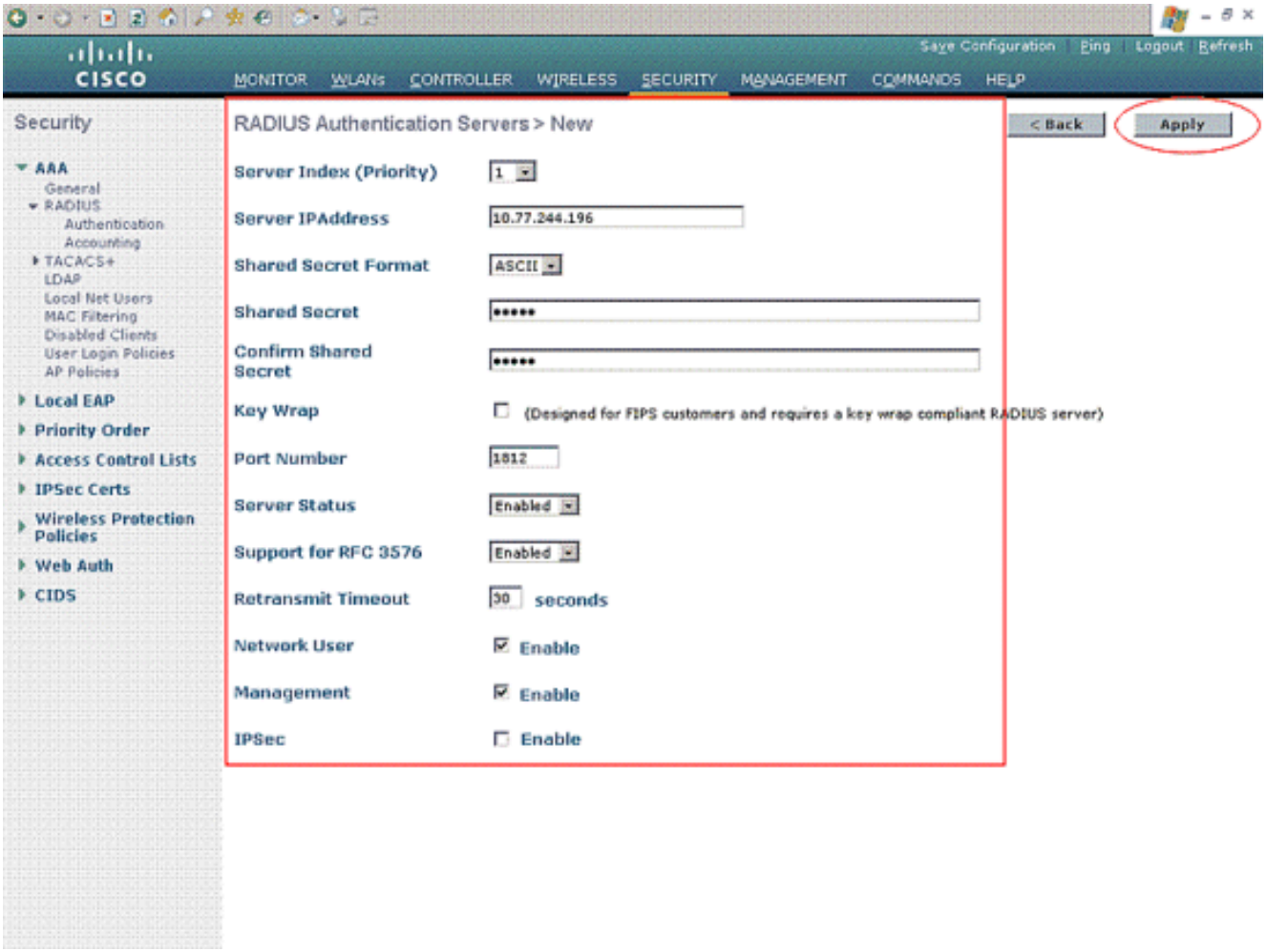
```
Office-VLAN
IP address: 172.16.1.25
Netmask: 255.255.0.0
Default gateway: 172.16.1.75 (sub-interface on Router R1)
Port on WLC: 1
DHCP server: 172.16.1.75
```

Configurazione del WLC per l'autenticazione con Cisco Secure ACS

Per inoltrare le credenziali dell'utente a un server RADIUS esterno (in questo caso, Cisco Secure ACS), è necessario configurare il WLC. Il server RADIUS convalida quindi le credenziali dell'utente e restituisce l'attributo del nome ACL al WLC al completamento dell'autenticazione dell'utente wireless.

Completare questa procedura per configurare il WLC per il server RADIUS:

1. Scegliere **Sicurezza** e **Autenticazione RADIUS** dall'interfaccia utente del controller per visualizzare la pagina **Server di autenticazione RADIUS**. Per definire un server RADIUS, fare clic su **New** (Nuovo).
2. Definire i parametri del server RADIUS nella pagina **Server di autenticazione RADIUS > Nuovo**. Questi parametri includono l'indirizzo IP, il segreto condiviso, il numero di porta e lo stato del server
RADIUS.

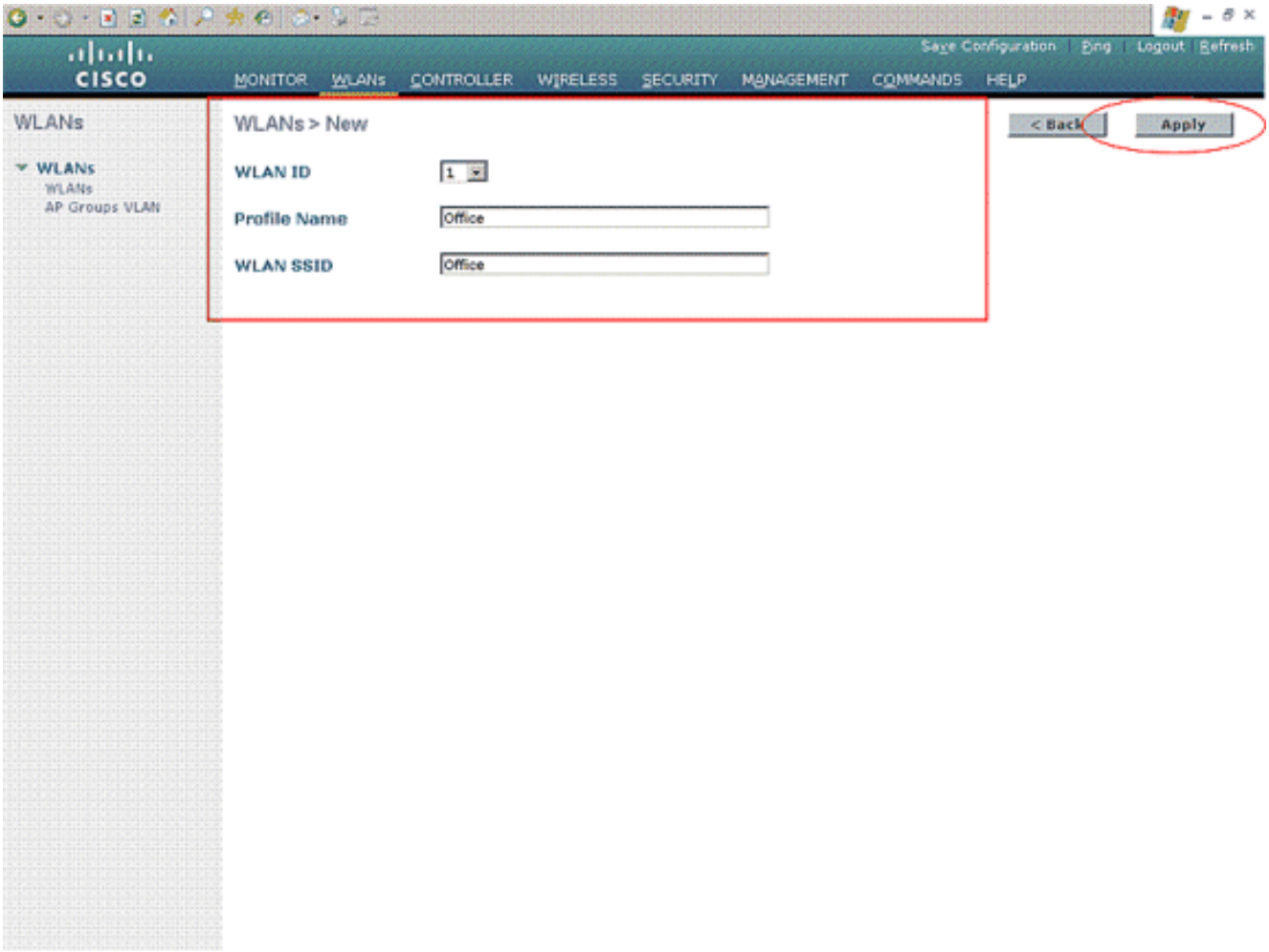


3. Le caselle di controllo **Utente di rete** e **Gestione** consentono di determinare se l'autenticazione basata su RADIUS è valida per la gestione e gli utenti della rete. In questo esempio viene utilizzato Cisco Secure ACS come server RADIUS con indirizzo IP 10.77.244.196. Fare clic su **Applica**.

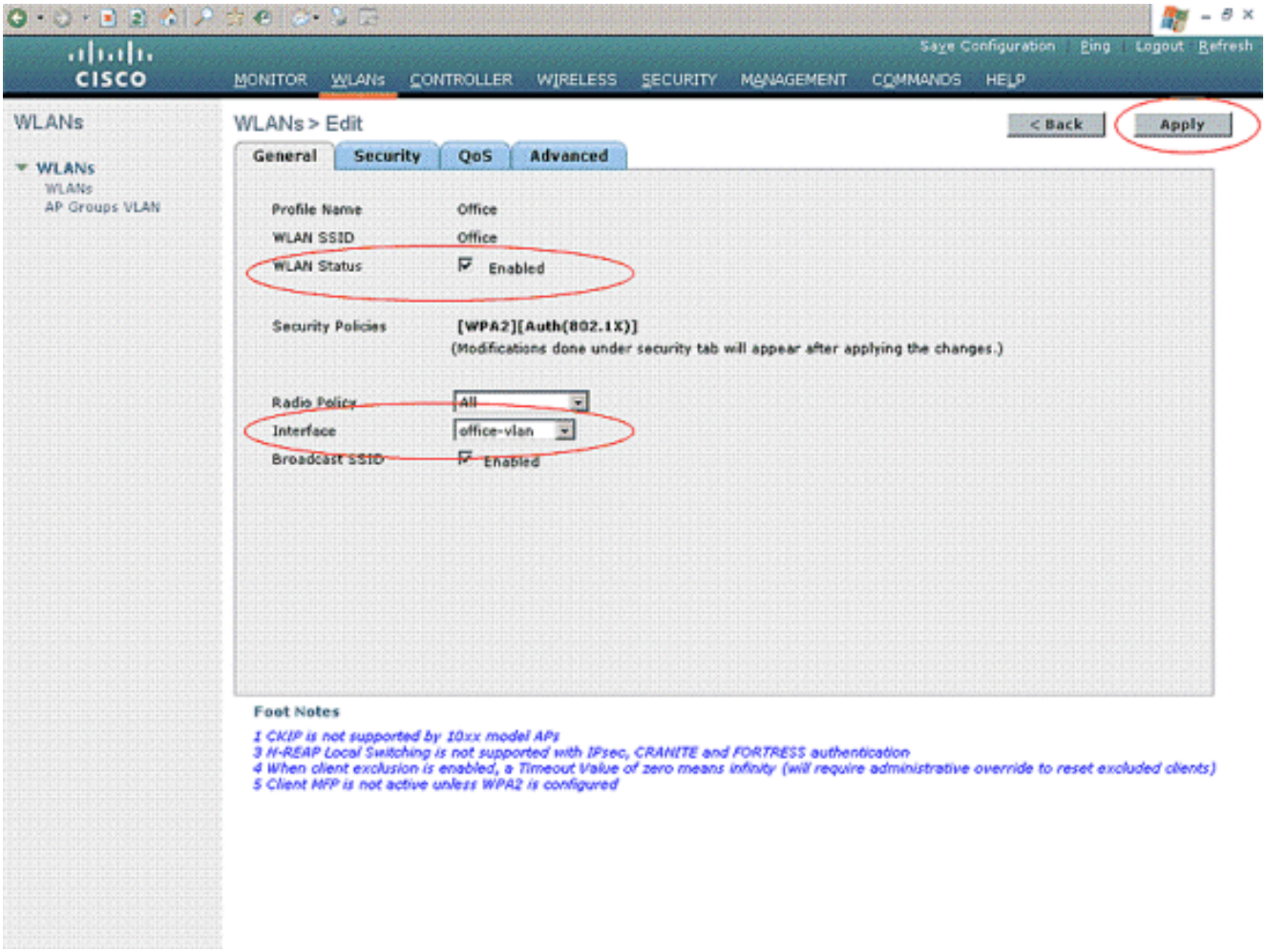
Creazione di una nuova WLAN per gli utenti wireless

Successivamente, è necessario creare una WLAN alla quale gli utenti wireless possano connettersi. Per creare una nuova WLAN, attenersi alla seguente procedura:

1. Dall'interfaccia utente del controller LAN wireless, fare clic su **WLAN**. In questa pagina vengono elencate le WLAN esistenti sul controller.
2. Per creare una nuova WLAN, scegliere **Nuovo**. Immettere l'ID WLAN, il nome del profilo e l'SSID WLAN per la WLAN, quindi fare clic su **Applica**. Per questa installazione, creare un **ufficio**
   WLAN.

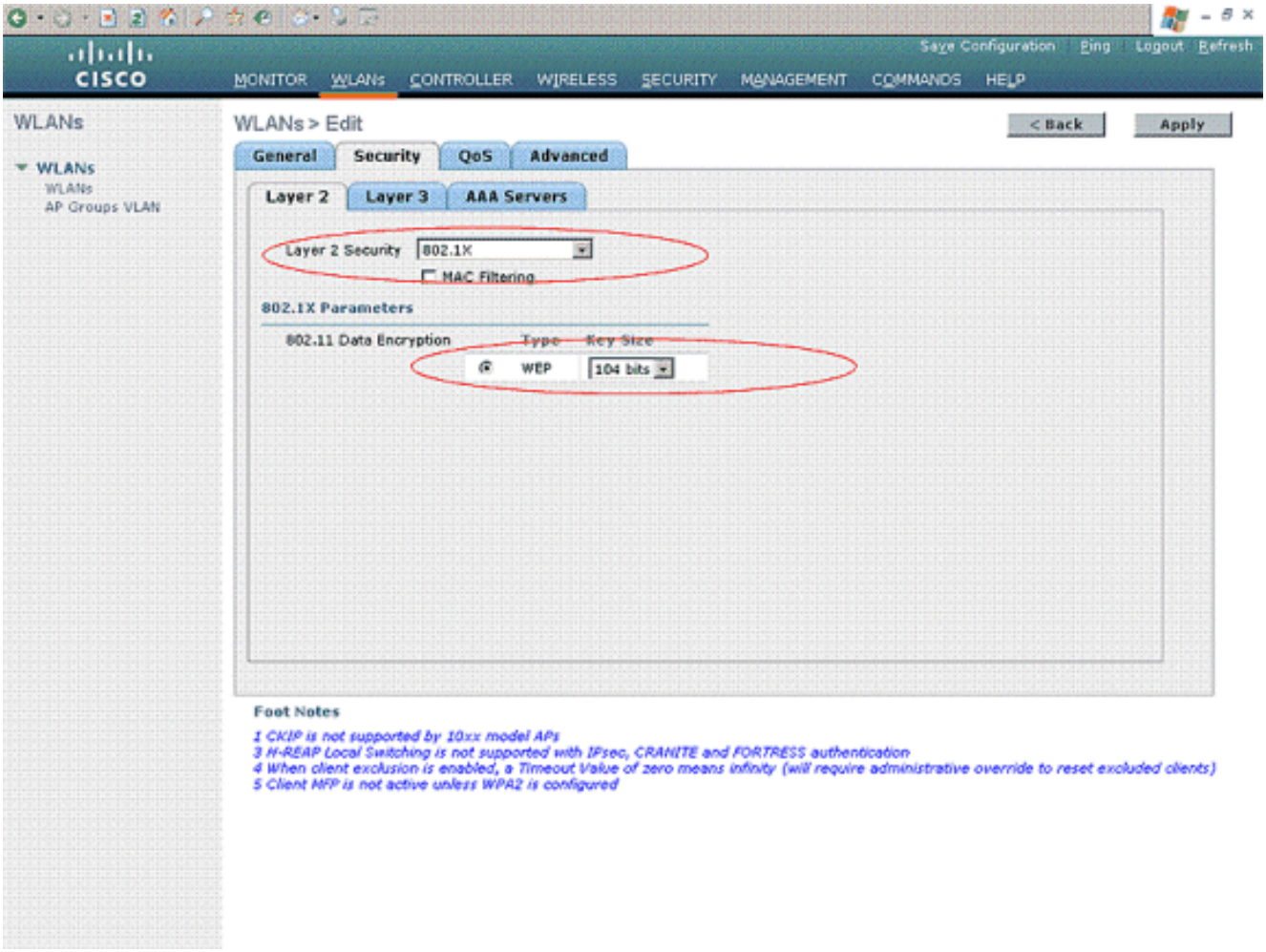


3. Dopo aver creato una nuova WLAN, viene visualizzata la pagina **WLAN > Modifica** per la nuova WLAN. In questa pagina è possibile definire vari parametri specifici per la WLAN, tra cui criteri generali, sicurezza, QoS e parametri avanzati.

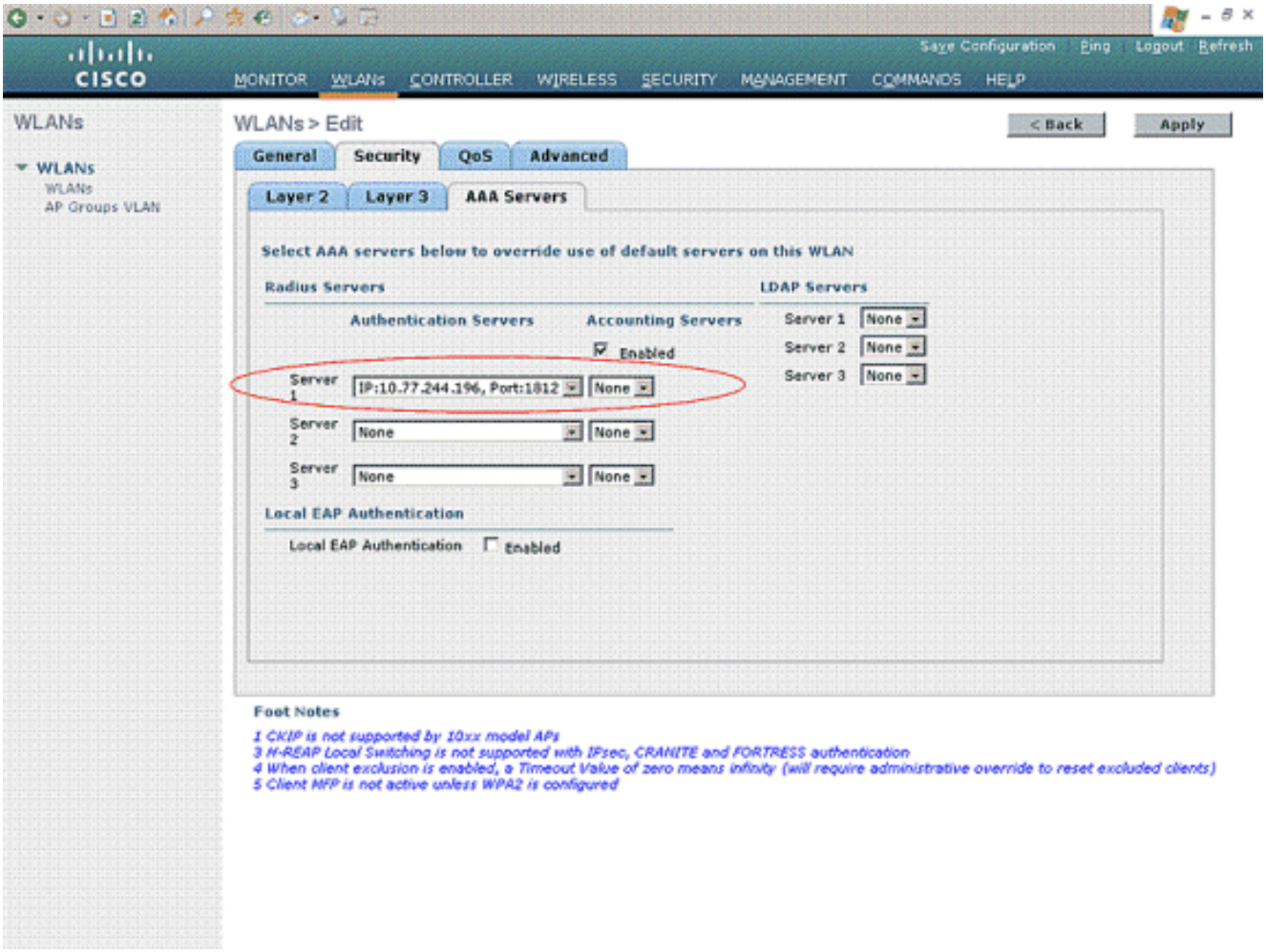


Per abilitare la WLAN, controllare **lo stato** della WLAN in Criteri generali. Selezionate l'interfaccia appropriata dal menu a discesa. Nell'esempio, usare l'interfaccia **Office-vlan**. Gli altri parametri di questa pagina possono essere modificati in base ai requisiti della rete WLAN.

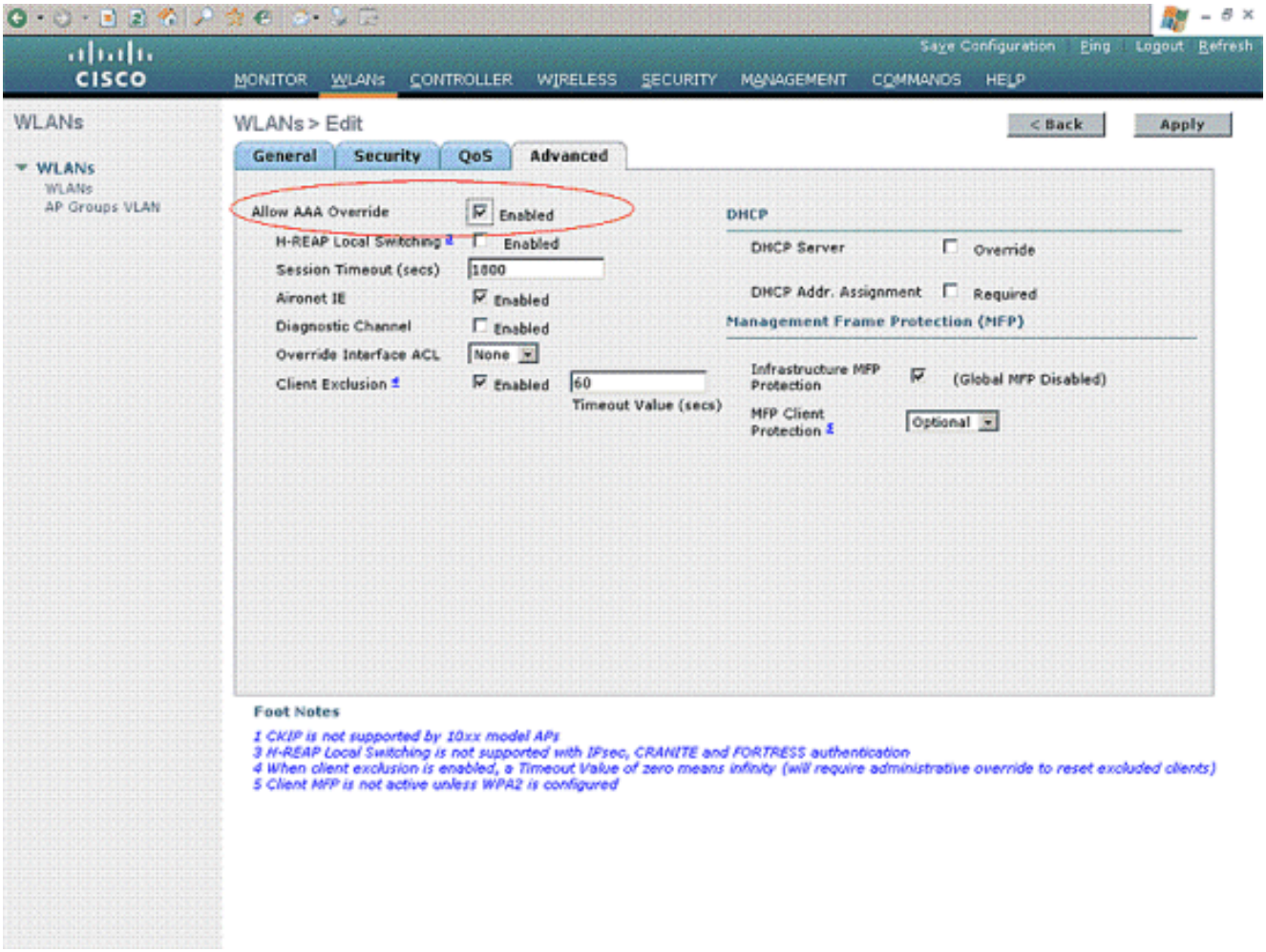
4. Scegliere la **scheda Protezione**. Scegliere **802.1x** dal menu a discesa Protezione di livello 2 (poiché si tratta di un'autenticazione LEAP). Scegliere la dimensione della chiave WEP appropriata in Parametri
802.1x.



5. Nella scheda Security (Sicurezza), selezionare la scheda secondaria del **server AAA**. Scegliere il server AAA utilizzato per autenticare i client wireless. Nell'esempio, usare il server ACS 10.77.244.196 per autenticare i client wireless.



6. Scegliere la scheda **Avanzate**. Selezionare **Consenti override AAA** per configurare la sostituzione dei criteri utente tramite AAA su una LAN wireless.



Quando l'override AAA è abilitato e un client ha parametri di autenticazione LAN wireless AAA e Cisco Wireless LAN Controller in conflitto, l'autenticazione del client viene eseguita dal server AAA. Nell'ambito di questa autenticazione, il sistema operativo sposta i client dalla VLAN LAN wireless predefinita della soluzione Cisco a una VLAN restituita dal server AAA e predefinita nella configurazione dell'interfaccia del controller LAN wireless Cisco, che si verifica solo se configurato per il filtro MAC, 802.1X e/o il funzionamento WPA. In tutti i casi, il sistema operativo usa anche i valori QoS, DSCP, tag di priorità 802.1p e ACL forniti dal server AAA, purché siano predefiniti nella configurazione dell'interfaccia del controller LAN wireless Cisco.

7. Scegliere gli altri parametri in base ai requisiti della rete. Fare clic su **Apply** (Applica).

Definizione degli ACL per gli utenti

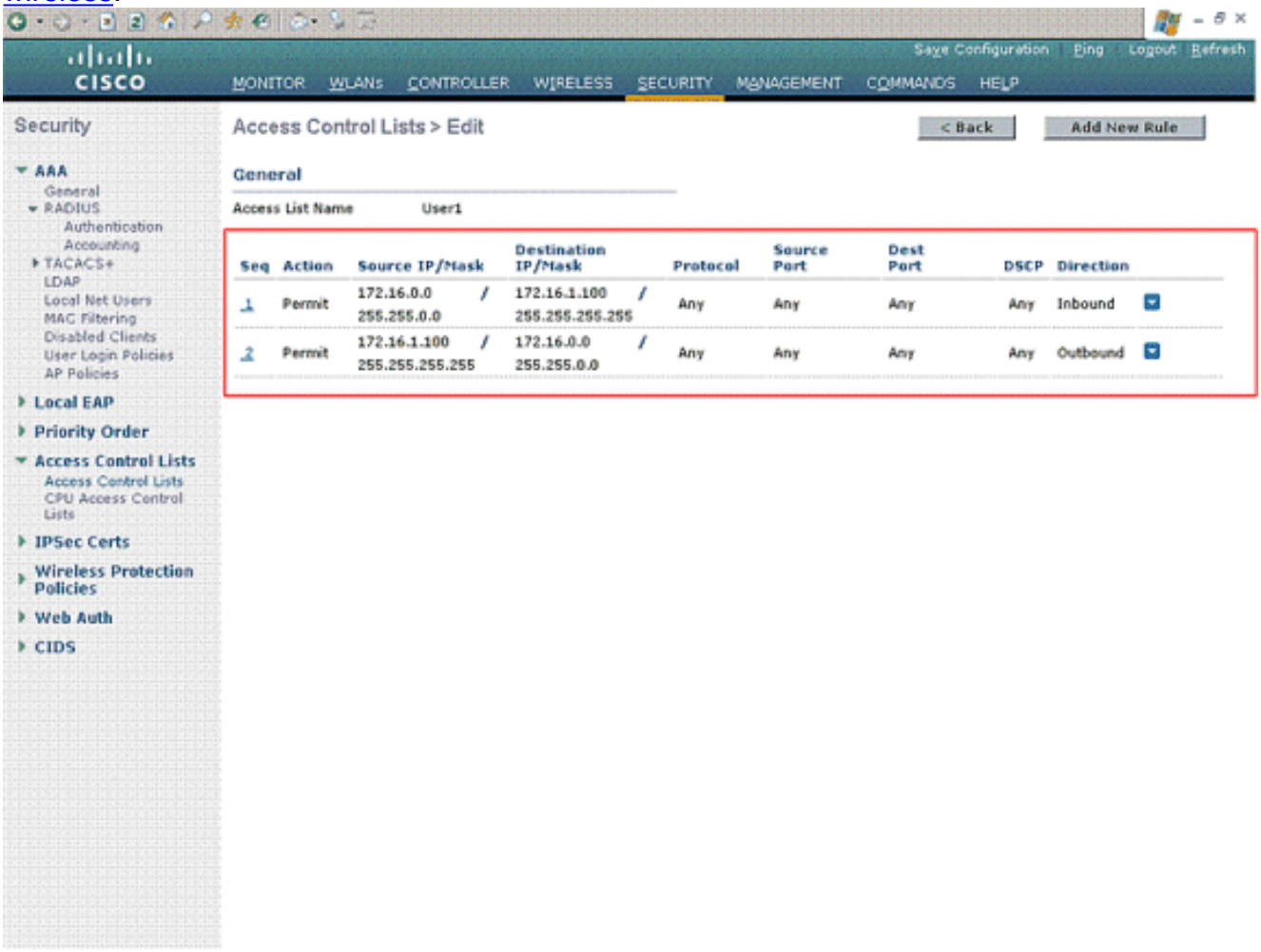
Per questa installazione, è necessario creare due ACL:

- ACL1: Per consentire all'utente 1 di accedere solo al server 172.16.1.100
- ACL2: Per consentire all'utente 2 di accedere solo al server 172.16.1.50

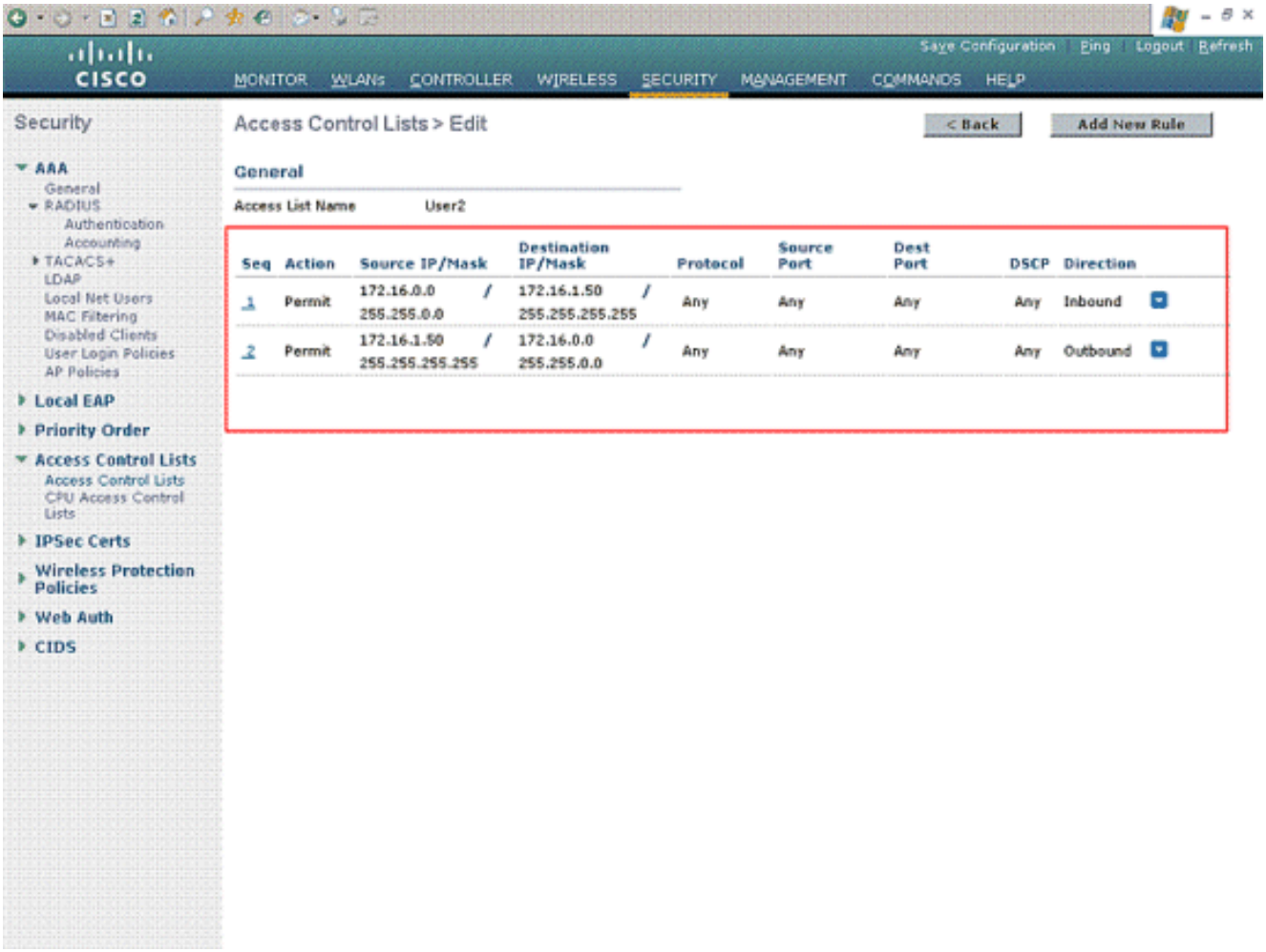
Completare questa procedura per configurare gli ACL sul WLC:

1. Dall'interfaccia utente del WLC, scegliere **Sicurezza > Access Control Lists**. Viene visualizzata la pagina Access Control Lists. In questa pagina vengono elencati gli ACL configurati sul WLC. Inoltre, permette di modificare o rimuovere gli ACL. Per creare un nuovo ACL, fare clic su **Nuovo**.
2. Questa pagina consente di creare nuovi ACL. Immettere il nome dell'ACL e fare clic su **Apply** (Applica). Dopo aver creato l'ACL, fare clic su **Edit** (Modifica) per creare le regole per l'ACL.

3. L'utente 1 deve essere in grado di accedere solo al server 172.16.1.100 e deve essere negato l'accesso a tutti gli altri dispositivi. Per questo, è necessario definire queste regole.Per ulteriori informazioni su come configurare gli ACL sui controller LAN wireless, consultare l'esempio di configurazione degli ACL sui controller LAN wireless.



4. Analogamente, è necessario creare un ACL per l'utente 2, che consenta all'utente 2 di accedere solo al server 172.16.1.50. ACL richiesto da User2.



Èstato configurato il controller LAN wireless per questa installazione. Il passaggio successivo è configurare il server Cisco Secure Access Control in modo che autentichi i client wireless e restituisca l'attributo Name dell'ACL al WLC una volta completata l'autenticazione.

Configurazione del server Cisco Secure ACS

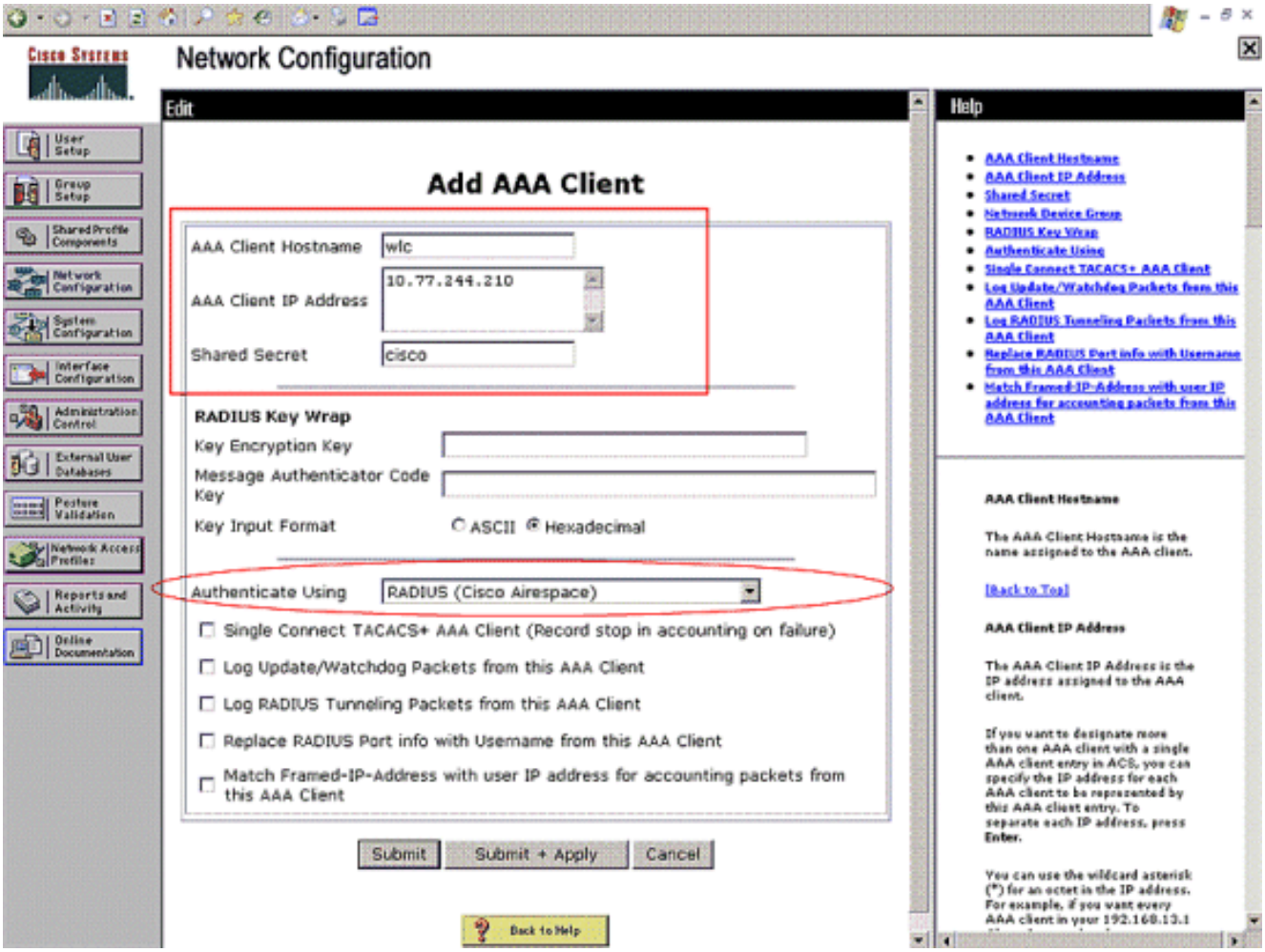
Affinché Cisco Secure ACS sia in grado di autenticare i client wireless, è necessario completare i seguenti passaggi:

- Configurare il controller LAN wireless come client AAA su Cisco Secure ACS.
- Configurare gli utenti e i profili utente su Cisco Secure ACS.

Configurazione del controller LAN wireless come client AAA su Cisco Secure ACS

Per configurare il controller LAN wireless come client AAA su Cisco Secure ACS, attenersi alla seguente procedura:

1. Fare clic su **Configurazione di rete > Aggiungi client AAA**. Viene visualizzata la pagina **Add AAA client**. In questa pagina, definire il nome del sistema WLC, l'indirizzo IP dell'interfaccia di gestione, il segreto condiviso e l'autenticazione tramite **Radius Airespace**. Di seguito è riportato un
esempio:



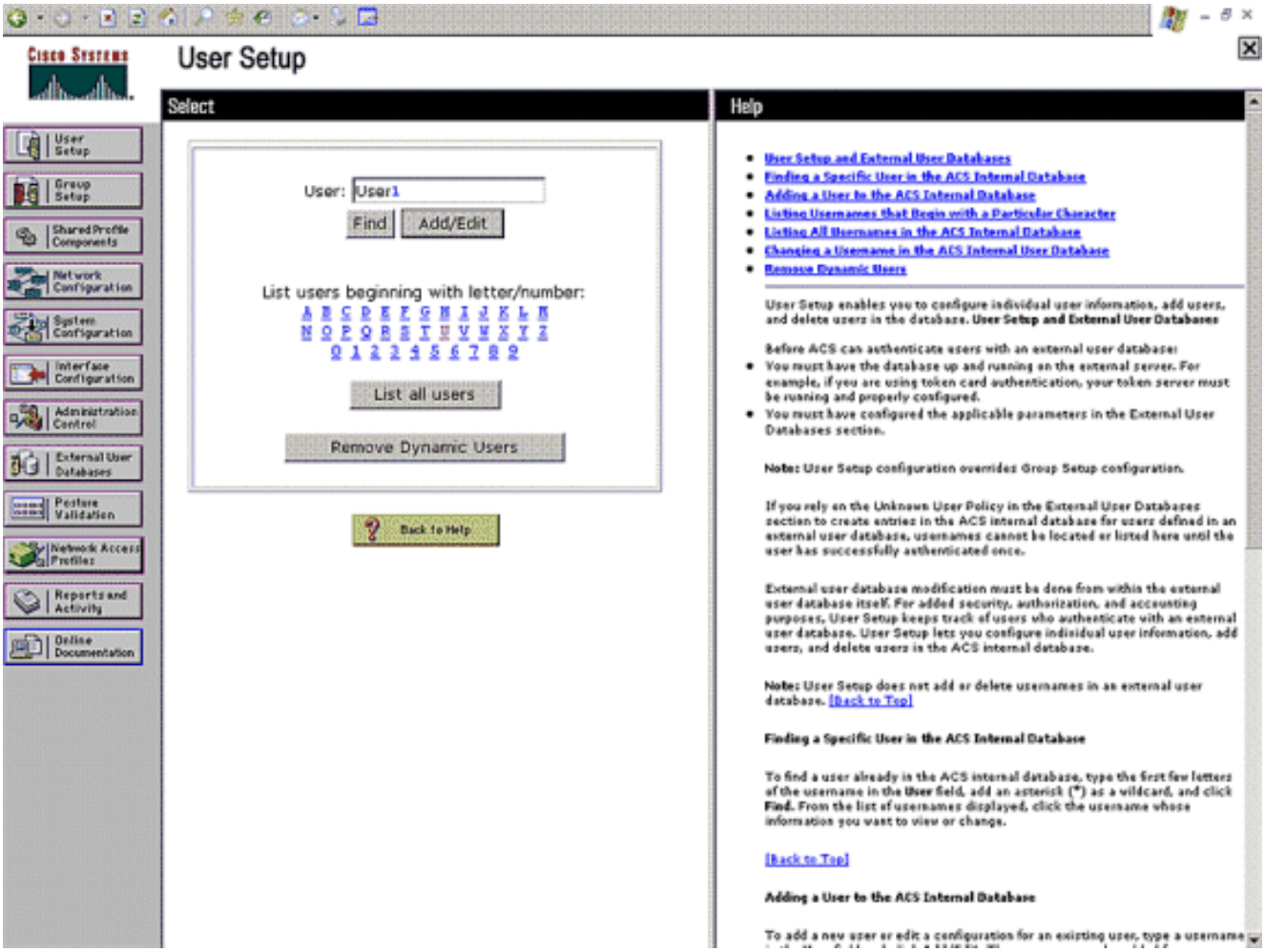
Nota: il segreto condiviso configurato su Cisco Secure ACS deve corrispondere al segreto condiviso configurato sul WLC in **Server di autenticazione RADIUS > Nuovo**.

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

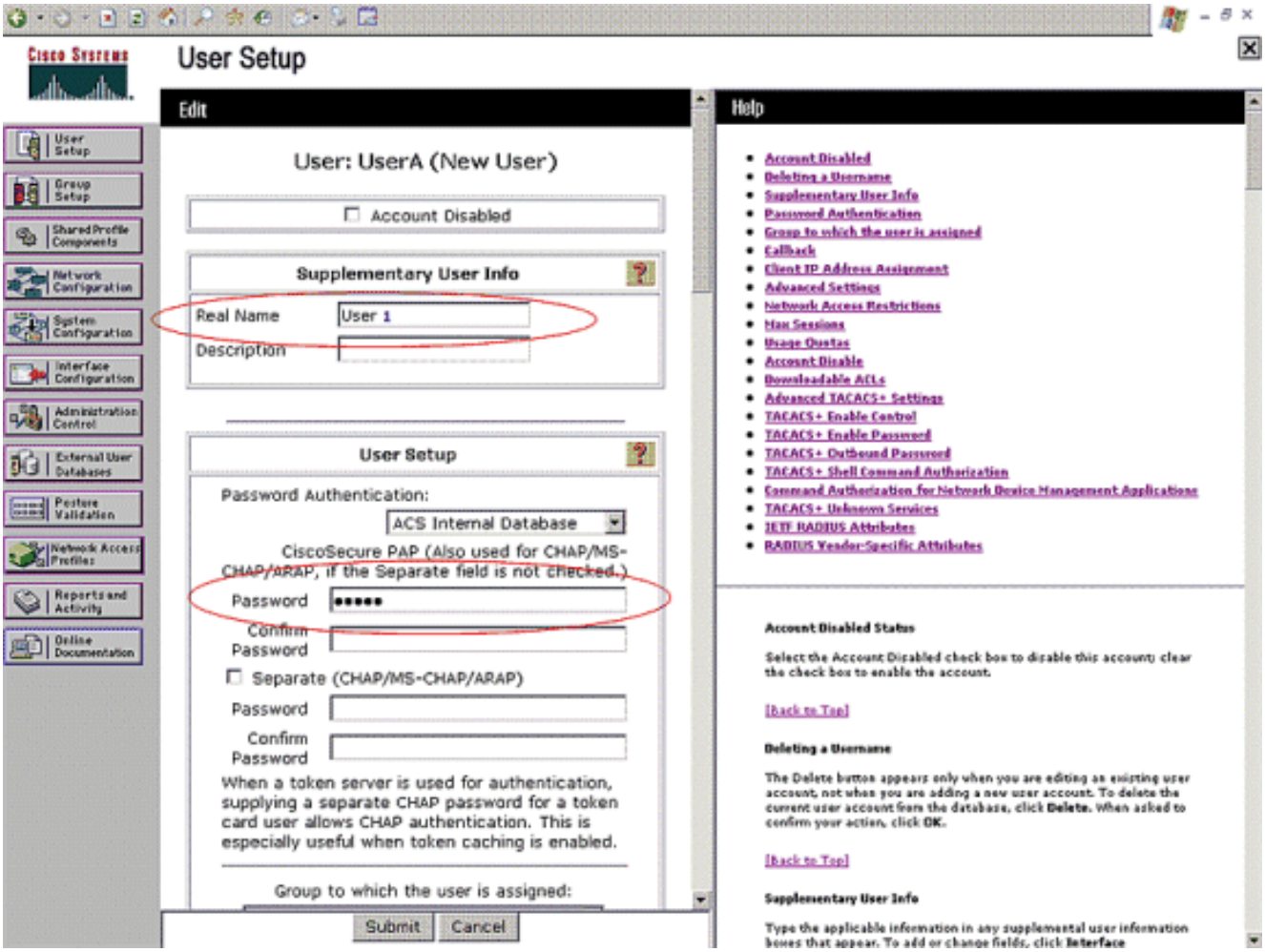
Configurazione di utenti e profili utente su Cisco Secure ACS

Per configurare gli utenti su Cisco Secure ACS, attenersi alla seguente procedura:

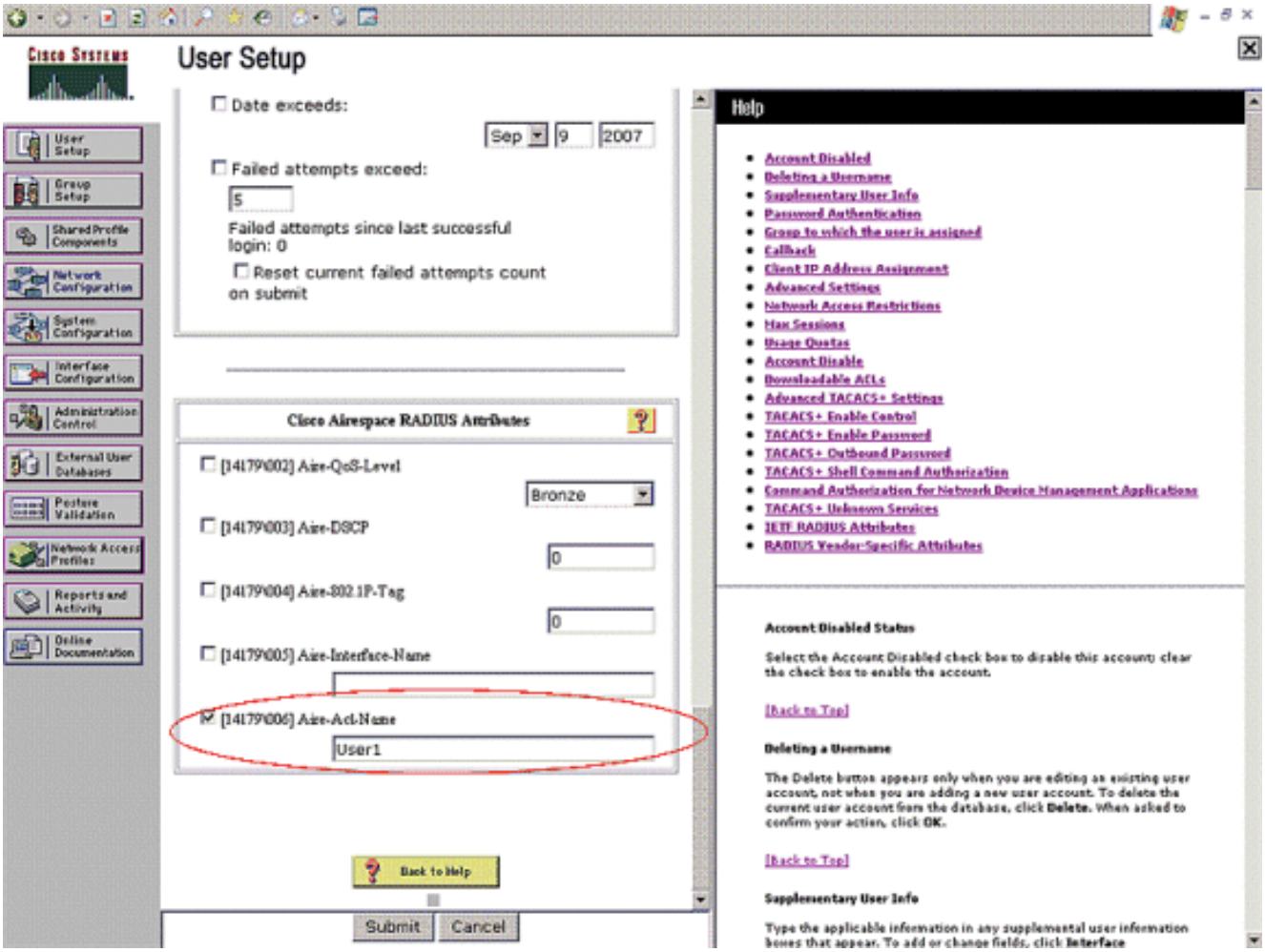
1. Selezionare **User Setup** (Configurazione utente) dall'interfaccia utente di ACS, immettere il nome utente e fare clic su **Add/Edit** (Aggiungi/Modifica). In questo esempio, l'utente è **User1**.



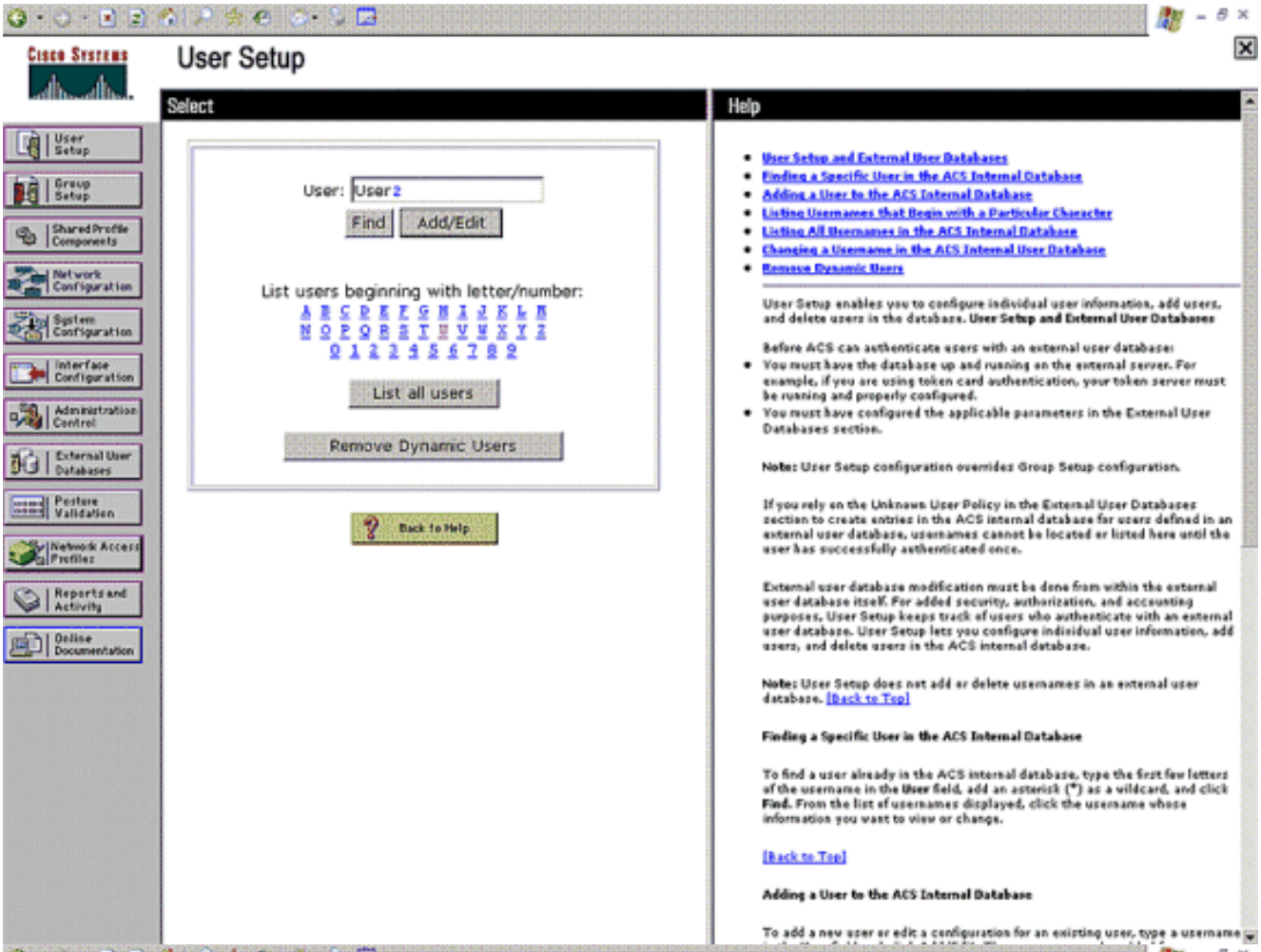
2. Quando viene visualizzata la pagina **Impostazione utente**, definire tutti i parametri specifici dell'utente. In questo esempio, gli attributi username, password, Supplementary User Information e RADIUS vengono configurati in quanto questi parametri sono necessari solo per l'autenticazione
EAP.

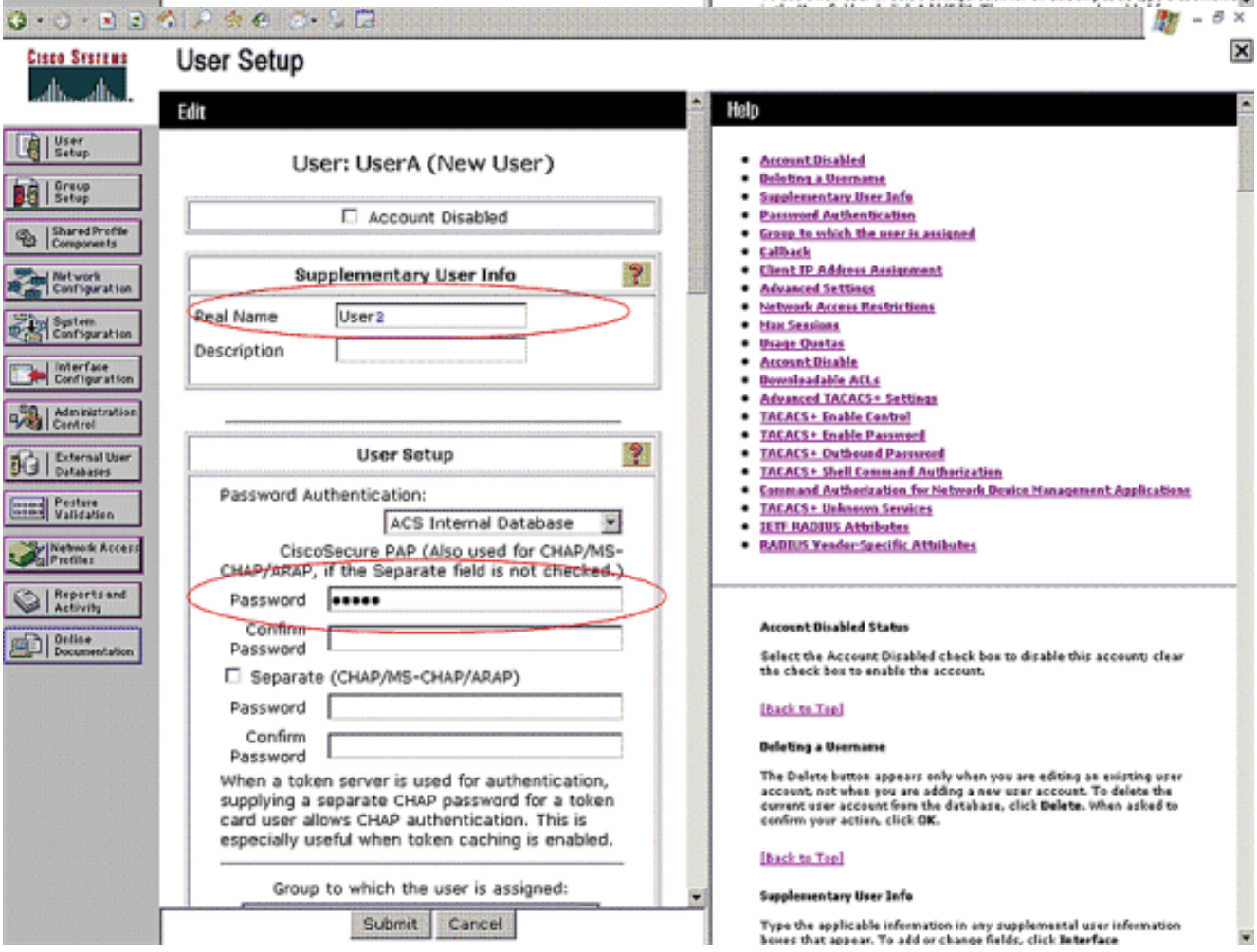


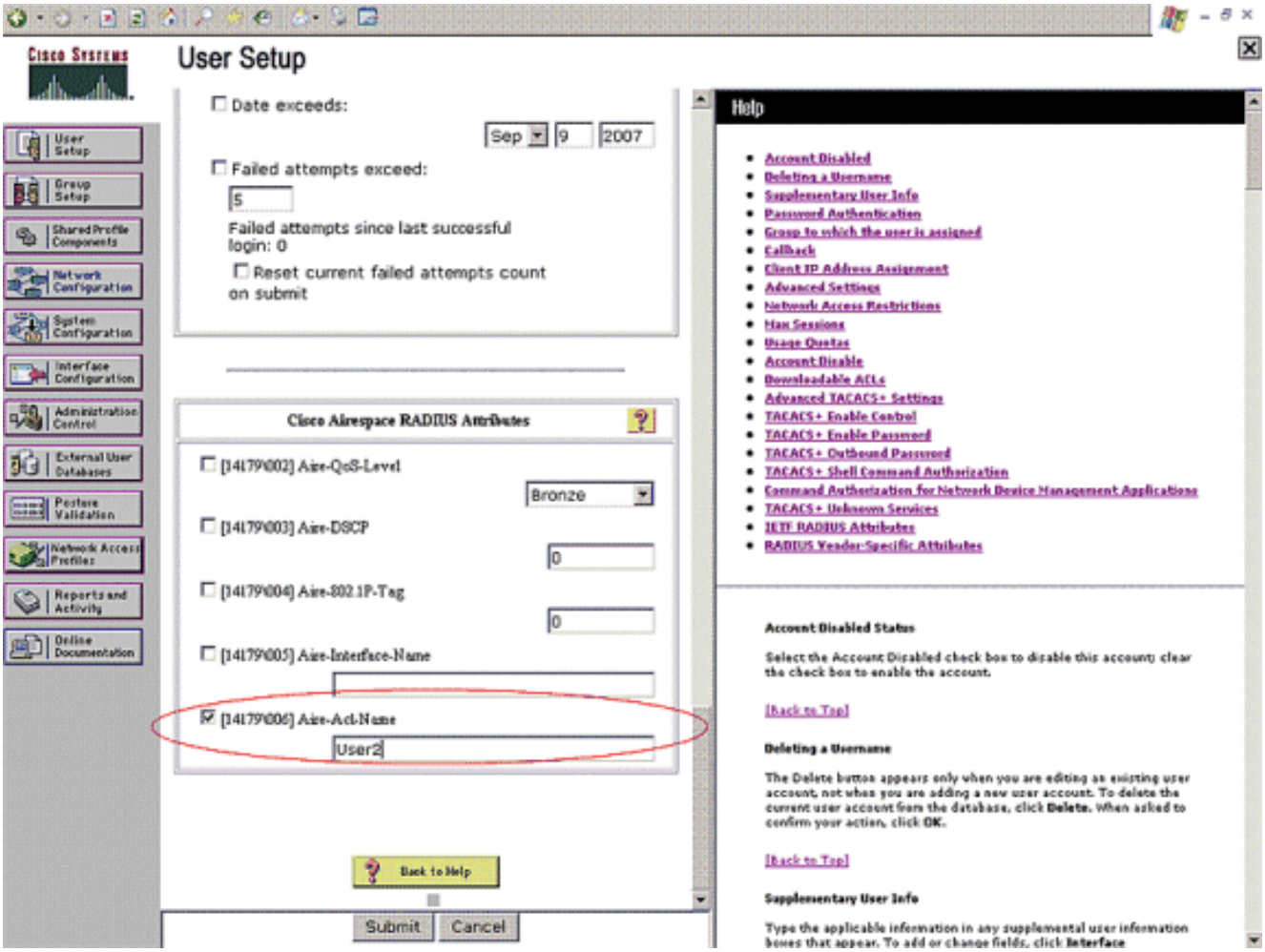
Scorrere verso il basso fino a visualizzare gli attributi Cisco Airespace RADIUS specifici dell'utente. Selezionare **Aire-ACL-Name** per abilitare l'ACS a restituire il nome ACL al WLC insieme alla risposta di autenticazione riuscita. Per l'utente 1, creare un ACL utente1 sul WLC. Immettere il nome ACL come
User1.



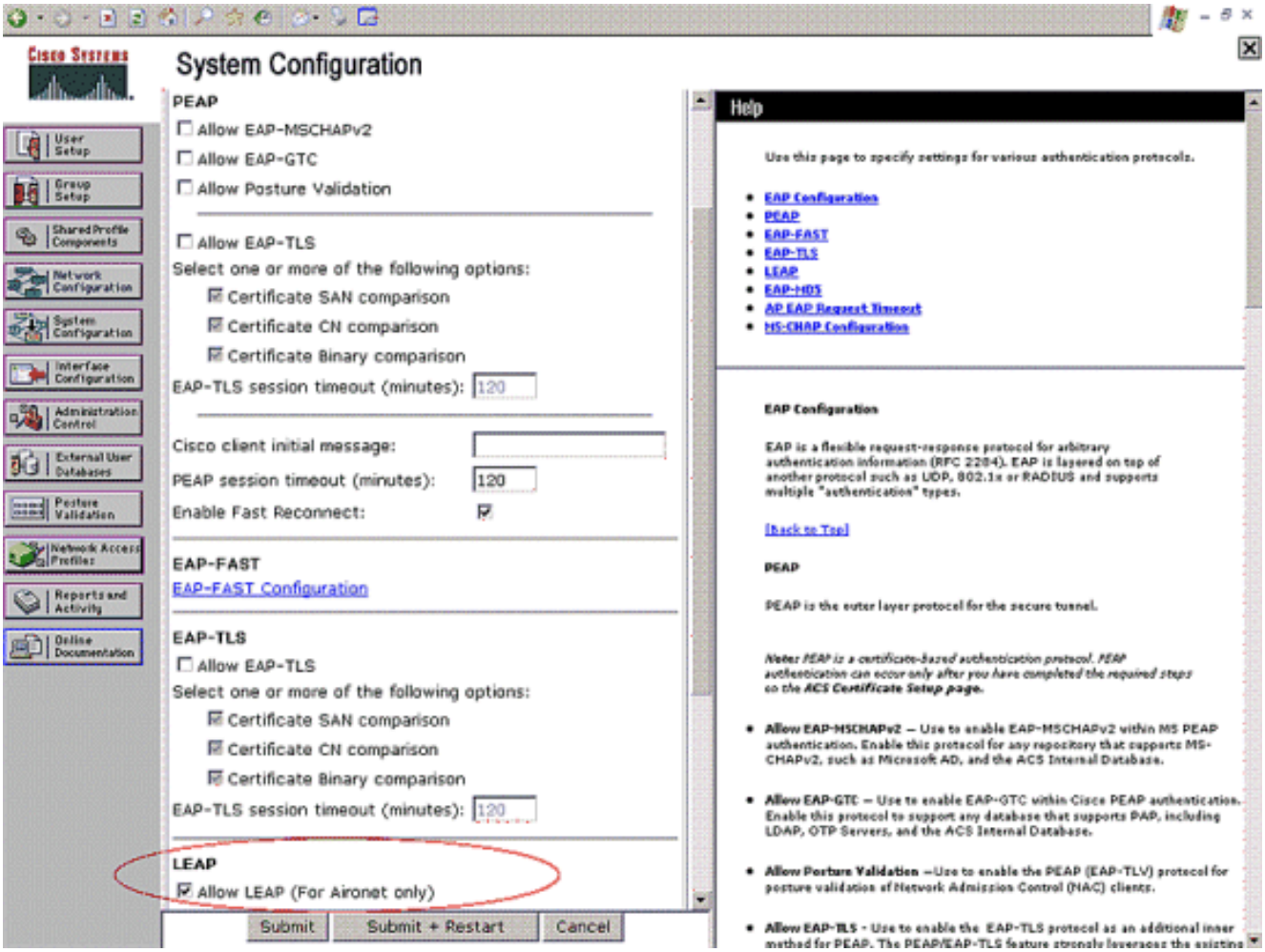
3. Ripetere la stessa procedura per creare User2, come mostrato di seguito.


Cisco Systems
User Setup
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
Online Documentation
Select
User: User2
Find
Add/Edit
List users beginning with letter/number:
A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
List all users
Remove Dynamic Users
Back to Help
Help
User Setup and External User Databases
Finding a Specific User in the ACS Internal Database
Adding a User to the ACS Internal Database
Listing Usernames that Begin with a Particular Character
Listing All Usernames in the ACS Internal Database
Changing a Username in the ACS Internal User Database
Remove Dynamic Users
User Setup enables you to configure individual user information, add users, and delete users in the database. User Setup and External User Databases
Before ACS can authenticate users with an external user database:
You must have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured.
You must have configured the applicable parameters in the External User Databases section.
Note: User Setup configuration overrides Group Setup configuration.
If you rely on the Unknown User Policy in the External User Databases section to create entries in the ACS internal database for users defined in an external user database, usernames cannot be located or listed here until the user has successfully authenticated once.
External user database modification must be done from within the external user database itself. For added security, authorization, and accounting purposes, User Setup keeps track of users who authenticate with an external user database. User Setup lets you configure individual user information, add users, and delete users in the ACS internal database.
Note: User Setup does not add or delete usernames in an external user database. [Back to Top]
Finding a Specific User in the ACS Internal Database
To find a user already in the ACS internal database, type the first few letters of the username in the User field, add an asterisk (*) as a wildcard, and click Find. From the list of usernames displayed, click the username whose information you want to view or change.
[Back to Top]
Adding a User to the ACS Internal Database
To add a new user or edit a configuration for an existing user, type a username


Cisco Systems
User Setup
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
Online Documentation
Edit
User: UserA (New User)
Account Disabled
Supplementary User Info
Real Name
User2
Description
User Setup
Password Authentication:
ACS Internal Database
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:
Submit
Cancel
Help
Account Disabled
Deleting a Username
Supplementary User Info
Password Authentication
Group to which the user is assigned
Callback
Client IP Address Assignment
Advanced Settings
Network Access Restrictions
Max Sessions
Usage Quotas
Account Disable
Downloadable ACLs
Advanced TACACS+ Settings
TACACS+ Enable Control
TACACS+ Enable Password
TACACS+ Outbound Password
TACACS+ Shell Command Authorization
Command Authorization for Network Device Management Applications
TACACS+ Unknown Services
IETF RADIUS Attributes
RADIUS Vendor-Specific Attributes
Account Disabled Status
Select the Account Disabled check box to disable this account; clear the check box to enable the account.
[Back to Top]
Deleting a Username
The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete. When asked to confirm your action, click OK.
[Back to Top]
Supplementary User Info
Type the applicable information in any supplemental user information boxes that appear. To add or change fields, click Interface



4. Fare clic su **Configurazione del sistema** e su **Configurazione autenticazione globale** per verificare che il server di autenticazione sia configurato in modo da eseguire il metodo di autenticazione EAP desiderato. In Impostazioni di configurazione EAP scegliere il metodo EAP appropriato. In questo esempio viene utilizzata l'autenticazione LEAP. Al termine, fare clic su **Submit**
(Invia).



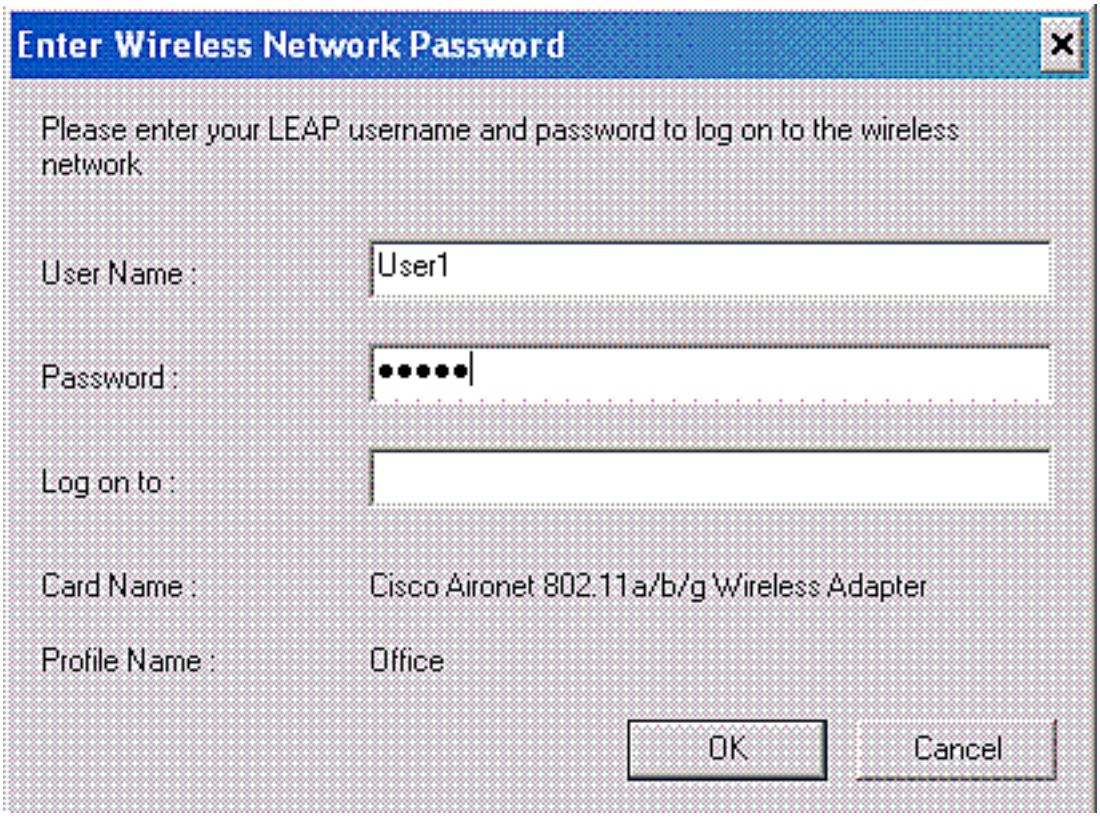
Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

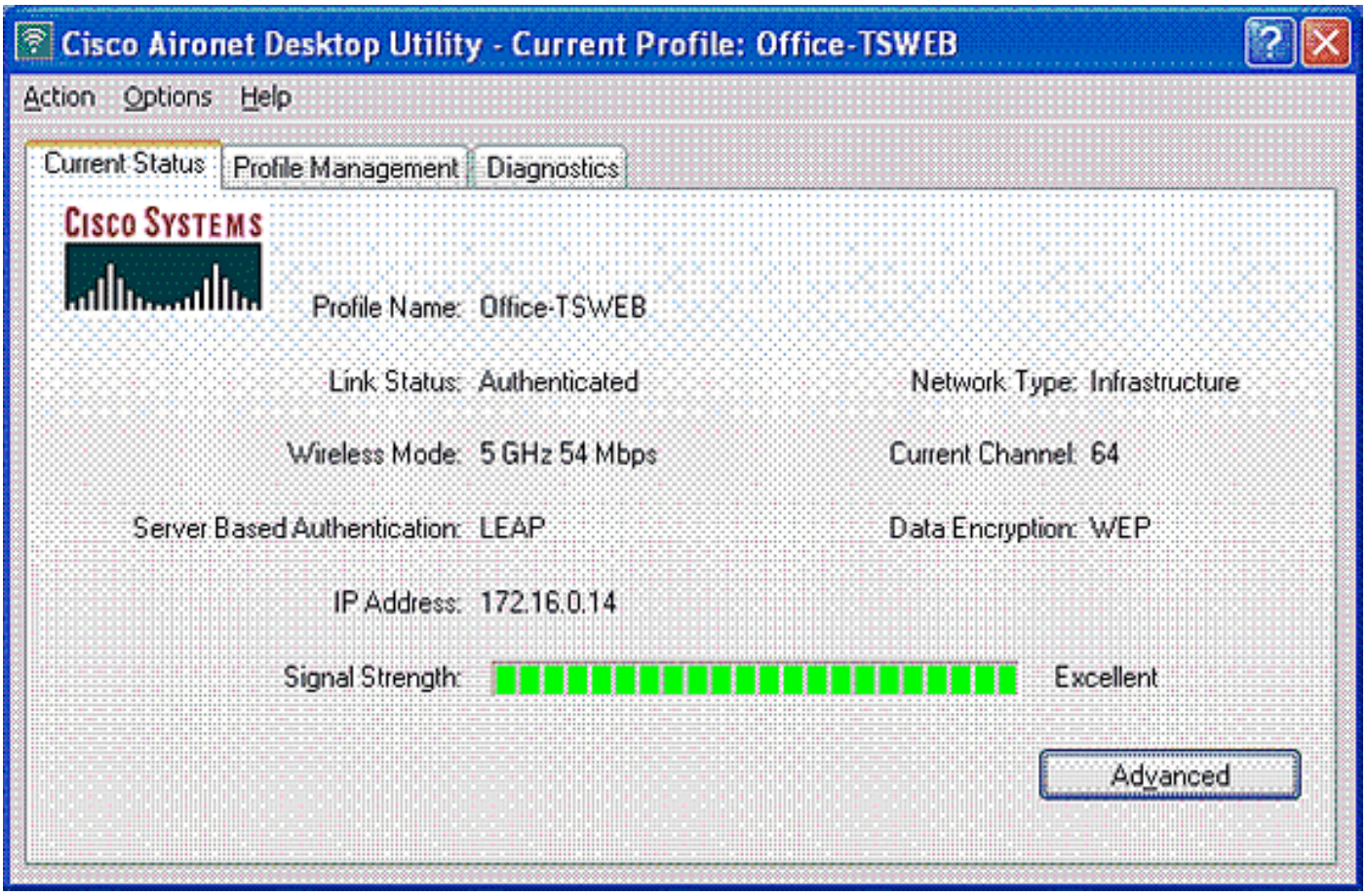
Per verificare se la configurazione funziona come previsto, associare un client wireless all'autenticazione LEAP del Lightweight AP.

Nota: in questo documento si presume che il profilo client sia configurato per l'autenticazione LEAP. Per ulteriori informazioni su come configurare l'adattatore client wireless 802.11 a/b/g per l'autenticazione LEAP, fare riferimento a Uso dell'autenticazione EAP.

Una volta attivato il profilo per il client wireless, all'utente viene richiesto di fornire il nome utente/password per l'autenticazione LEAP. Questo è ciò che accade quando l'utente 1 tenta di autenticarsi al LAP.



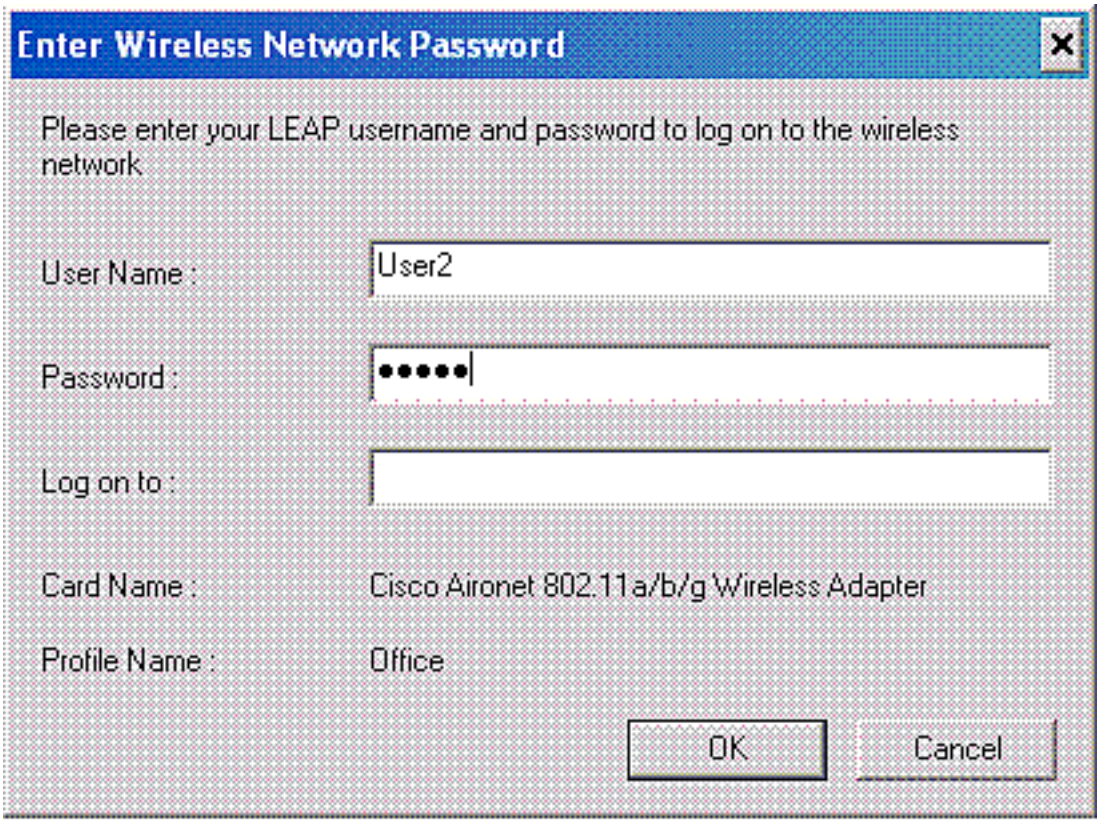
Il Lightweight AP e quindi il WLC passano le credenziali dell'utente al server RADIUS esterno (Cisco Secure ACS) per convalidarle. Il server RADIUS confronta i dati con il database degli utenti e, se l'autenticazione ha esito positivo, restituisce al WLC il nome ACL configurato per l'utente. In questo caso, l'ACL User1 viene restituito al WLC.

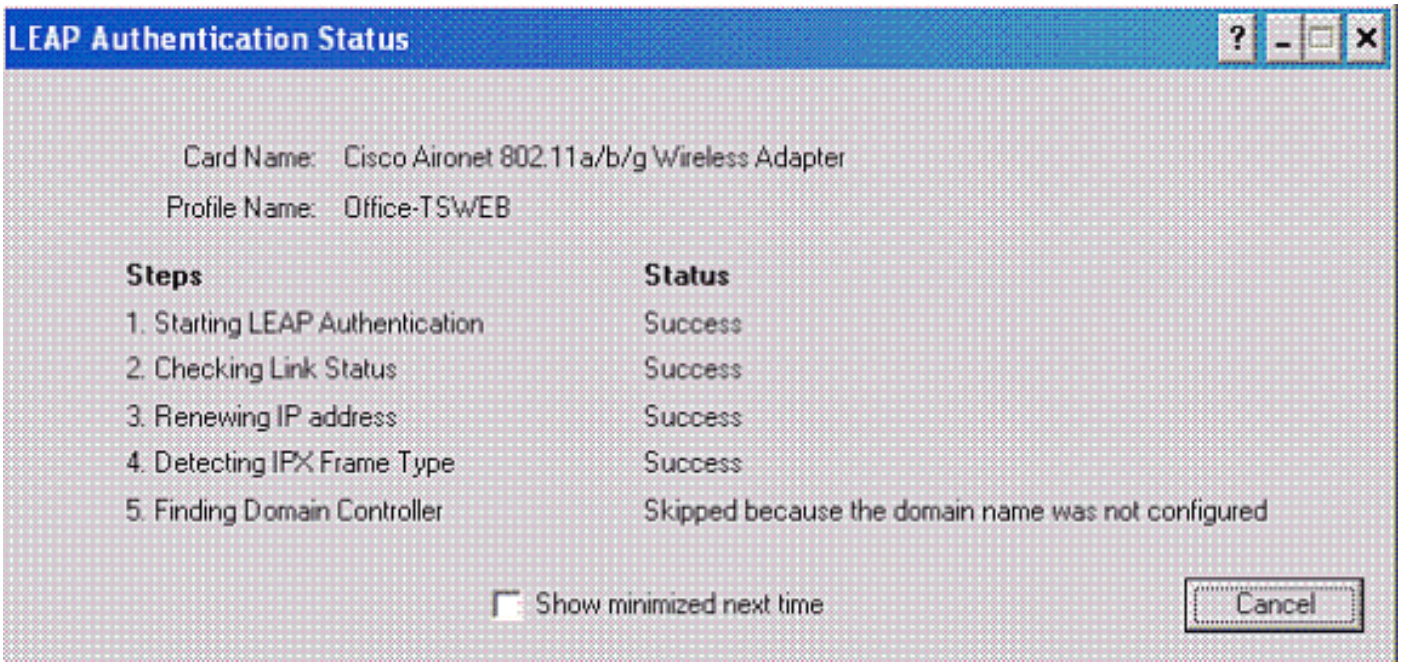


Il controller LAN wireless applica questo ACL all'utente 1. Questo output del ping indica che l'utente 1 è in grado di accedere solo al server 172.16.1.100, ma non a qualsiasi altra periferica.

```
D:\Documents and Settings\Administrator>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:

Reply from 172.16.1.100: bytes=32 time=3ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255
Reply from 172.16.1.100: bytes=32 time=1ms TTL=255

Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms

D:\Documents and Settings\Administrator>ping 172.16.1.50

Pinging 172.16.1.50 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.50:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Analogamente, quando l'utente 2 tenta di accedere alla WLAN, il server RADIUS, una volta completata l'autenticazione, restituisce l'ACL utente 2 al WLC.





Il controller LAN wireless applica questo ACL all'utente 2. Questo output del ping indica che l'utente 2 è in grado di accedere solo al server 172.16.1.50, ma non a qualsiasi altra periferica.

```
D:\Documents and Settings\Administrator>ping 172.16.1.50

Pinging 172.16.1.50 with 32 bytes of data:

Reply from 172.16.1.50: bytes=32 time=3ms TTL=255
Reply from 172.16.1.50: bytes=32 time=18ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255

Ping statistics for 172.16.1.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 18ms, Average = 5ms

D:\Documents and Settings\Administrator>ping 172.16.1.100

Pinging 172.16.1.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Risoluzione dei problemi

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

Sul controller LAN wireless, è possibile usare questi comandi di debug anche per risolvere i problemi di autenticazione AAA

- **debug aaa all enable**: configura il debug di tutti i messaggi AAA
- **debug dot1x packet enable**: abilita il debug di tutti i pacchetti dot1x
- **debug client <indirizzo MAC>**: abilita il debug dei client wireless

Di seguito è riportato un esempio del comando **debug aaa all enable**

Nota: alcune delle linee nell'output sono state spostate nella seconda linea a causa dei vincoli di spazio.

```
Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104
Thu Aug 16 14:42:54 2007:       Callback.................0x85ed228
Thu Aug 16 14:42:54 2007:       protocolType.............0x00140001
Thu Aug 16 14:42:54 2007:       proxyState...............00:40:96:AF:3E:93-03:01
Thu Aug 16 14:42:54 2007:       Packet contains 16 AVPs (not shown)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Successful transmission of Authentication Packet
   (id 1) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00
Thu Aug 16 14:42:54 2007: 00000000: 01 01 00 d0 2d 34 f5 99  b4 19 27 28 eb 5f 35 9c
   ....-4....'(._5.
Thu Aug 16 14:42:54 2007: 00000010: 8f a9 00 dd 01 07 75 73  65 72 31 1f 13 30 30 2d
   ......user1..00-
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46  2d 33 45 2d 39 33 1e 20
   40-96-AF-3E-93..
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35  2d 35 42 2d 46 42 2d 44
   00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65  2d 54 53 57 45 42 05 06
   0:Office-TSWEB..
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d  f4 d2 20 05 77 6c 63 1a
   .......M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00  00 00 01 06 06 00 00 00
   ...7c...........
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d  06 00 00 00 13 40 06 00
   .......=.....@..
Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00  06 51 04 32 30 4f 27 02
   ...A.....Q.20O'.
Thu Aug 16 14:42:54 2007: 00000090: 01 00 25 11 01 00 18 1d  87 9d 0b f9 dd e5 39 0d
   ..%...........9.
Thu Aug 16 14:42:54 2007: 000000a0: 2e 82 eb 17 c6 23 b7 96  dc c3 55 ff 7c 51 4e 75
   .....#....U.|QNu
Thu Aug 16 14:42:54 2007: 000000b0: 73 65 72 31 18 0a 53 56  43 3d 30 2e 31 3b 50 12
   ser1..SVC=0.1;P.
Thu Aug 16 14:42:54 2007: 000000c0: 1a d5 3b 35 5e 93 11 c0  c6 2f 5e f5 65 e9 3e 2d
   ..;5^..../^.e.>-
Thu Aug 16 14:42:54 2007: 00000000: 0b 01 00 36 8c 31 6a b4  27 e6 d4 0e 1b 8e 5d 19
   ...6.1j.'.....].
Thu Aug 16 14:42:54 2007: 00000010: 60 1c c2 16 4f 06 03 01  00 04 18 0a 53 56 43 3d
   ...O.......SVC=
Thu Aug 16 14:42:54 2007: 00000020: 30 2e 31 3b 50 12 6c fb  90 ec 48 9b fb d7 ce ca
   0.1;P.l...H.....
Thu Aug 16 14:42:54 2007: 00000030: 3b 64 93 10 fe 09      ;d....
Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=11
Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=11
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Access-Challenge received from RADIUS server
   10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
Thu Aug 16 14:42:54 2007:       structureSize............104
Thu Aug 16 14:42:54 2007:       resultCode...............255
Thu Aug 16 14:42:54 2007:       protocolUsed.............0x00000001
Thu Aug 16 14:42:54 2007:       proxyState...............
   00:40:96:AF:3E:93-03:01
```

```
Thu Aug 16 14:42:54 2007:       Packet contains 3 AVPs (not shown)
Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xb1ab104
Thu Aug 16 14:42:54 2007:       Callback.................0x85ed228
Thu Aug 16 14:42:54 2007:       protocolType.............0x00140001
Thu Aug 16 14:42:54 2007:       proxyState.......................
   00:40:96:AF:3E:93-03:02
Thu Aug 16 14:42:54 2007:       Packet contains 16 AVPs (not shown)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Successful transmission of Authentication Packet (id 2) to 10.77.244.196:1812,
proxy state 00:40:96:af:3e:93-00:00
Thu Aug 16 14:42:54 2007: 00000000: 01 02 00 c0 38 b6 b2 20  ff 5b f2 16 64 df 02 61
   ....8....[..d..a
Thu Aug 16 14:42:54 2007: 00000010: cf f5 93 4b 01 07 75 73  65 72 31 1f 13 30 30 2d
   ...K..User1..00-
Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46  2d 33 45 2d 39 33 1e 20
   40-96-AF-3E-93..
Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35  2d 35 42 2d 46 42 2d 44
   00-0B-85-5B-FB-D
Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65  2d 54 53 57 45 42 05 06
   0:Office..
Thu Aug 16 14:42:54 2007: 00000050: 00 00 00 01 04 06 0a 4d  f4 d2 20 05 77 6c 63 1a
   .......M....wlc.
Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00  00 00 01 06 06 00 00 00
   ...7c...........
Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d  06 00 00 00 13 40 06 00
   .......=.....@..
Thu Aug 16 14:42:54 2007: 00000080: 00 00 0d 41 06 00 00 00  06 51 04 32 30 4f 17 01
   ...A.....Q.20O..
Thu Aug 16 14:42:54 2007: 00000090: 01 00 15 11 01 00 08 0f  14 05 65 1b 28 61 c9 75
   ..........e.(a.u
Thu Aug 16 14:42:54 2007: 000000a0: 73 65 72 31 18 0a 53 56  43 3d 30 2e 31 3b 50 12
   ser1..SVC=0.1;P.
Thu Aug 16 14:42:54 2007: 000000b0: 05 ba 6b af fe a4 b0 d1  a2 94 f8 39 80 ca 3c 96
   ..k........9..<.
Thu Aug 16 14:42:54 2007: 00000000: 02 02 00 ce c9 3d 5d c8  6c 07 8e fb 58 84 8d f6
   .....=].l...X...
Thu Aug 16 14:42:54 2007: 00000010: 33 6d 93 21 08 06 ff ff  ff ff 4f 27 02 01 00 25
   3m.!......O'...%
Thu Aug 16 14:42:54 2007: 00000020: 11 01 00 18 e5 e5 31 1e  33 b5 4e 69 90 e7 84 25
   ......1.3.Ni...%
Thu Aug 16 14:42:54 2007: 00000030: 42 a9 20 ac 84 33 9f 87  ca dc c9 b3 75 73 65 72
   B....3......user
Thu Aug 16 14:42:54 2007: 00000040: 31 1a 3b 00 00 00 09 01  35 6c 65 61 70 3a 73 65
   1.;.....5leap:se
Thu Aug 16 14:42:54 2007: 00000050: 73 73 69 6f 6e 2d 6b 65  79 3d 29 80 1d 2c 1c 85
   ssion-key=)..,..
Thu Aug 16 14:42:54 2007: 00000060: db 1c 29 7e 40 8a b8 93  69 2a 55 d2 e5 46 89 8b
   ..)~@...i*U..F..
Thu Aug 16 14:42:54 2007: 00000070: 2c 3b 65 49 3e 44 cf 7e  95 29 47 54 1a 1f 00 00
   ,;eI>D.~.)GT....
Thu Aug 16 14:42:54 2007: 00000080: 00 09 01 19 61 75 74 68  2d 61 6c 67 6f 2d 74 79
   ....auth-algo-ty
Thu Aug 16 14:42:54 2007: 00000090: 70 65 3d 65 61 70 2d 6c  65 61 70 1a 0d 00 00 37
   pe=eap-leap....7
Thu Aug 16 14:42:54 2007: 000000a0: 63 06 07 55 73 65 72 31  19 14 43 41 43 53 3a 30
   c..User1..CACS:0
Thu Aug 16 14:42:54 2007: 000000b0: 2f 39 2f 61 34 64 66 34  64 32 2f 31 50 12 9a 71
   /9/a4df4d2/1P..q
Thu Aug 16 14:42:54 2007: 000000c0: 09 99 7d 74 89 ad af e5  c8 b1 71 94 97 d1
   ..}t......q...
Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=2
Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=2
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
Access-Accept received from RADIUS server
```

```
   10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3
Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800
Thu Aug 16 14:42:54 2007:       structureSize............236
Thu Aug 16 14:42:54 2007:       resultCode...............0
Thu Aug 16 14:42:54 2007:       protocolUsed.............0x0
0000001
Thu Aug 16 14:42:54 2007:       proxyState...............00:
40:96:AF:3E:93-03:02
Thu Aug 16 14:42:54 2007:  Packet contains 6 AVPs:
Thu Aug 16 14:42:54 2007:  AVP[01] Framed-IP-Address..........0xffffffff (-1)
   (4 bytes)
Thu Aug 16 14:42:54 2007:  AVP[02] EAP-Message................DATA (37 bytes)
Thu Aug 16 14:42:54 2007:  AVP[03] Cisco / LEAP-Session-Key...DATA (16 bytes)
Thu Aug 16 14:42:54 2007:  AVP[04] Airespace / ACL-Name.......User1 (5 bytes)
Thu Aug 16 14:42:54 2007:  AVP[05] Class......................CACS:0/9/a4df4d2/1
   (18 bytes)
Thu Aug 16 14:42:54 2007:  AVP[06] Message-Authenticator......DATA (16 bytes)
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Applying new AAA override
   for station 00:40:96:af:3e:93
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Override values
   for station 00:40:96:af:3e:93
               source: 4, valid bits: 0x400
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                      vlanIfName: '',
aclName:User1
Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93
   Inserting new RADIUS override into chain for station 00:40:96:af:3e:93
```

Per riconoscere le WLAN che usano l'autenticazione del server RADIUS, è possibile usare una combinazione del comando **show wlan summary**. Quindi, è possibile visualizzare il comando **show client summary** per verificare quali indirizzi MAC (client) sono stati autenticati correttamente sulle WLAN RADIUS. È inoltre possibile correlare questa condizione ai log dei tentativi passati o non riusciti di Cisco Secure ACS.

Cisco consiglia di provare le configurazioni ACL con un client wireless per verificare che siano state configurate correttamente. Se l'ACL non funziona correttamente, verificare gli ACL sulla pagina Web dell'ACL e verificare che le modifiche all'ACL siano state applicate all'interfaccia del controller.

Per verificare la configurazione, è possibile anche utilizzare i seguenti comandi show:

- **show acl summary**: per visualizzare gli ACL configurati sul controller, usare il comando **show acl summary**.

Di seguito è riportato un esempio:

```
(Cisco Controller) >show acl summary

ACL Name                          Applied
--------------------------------- -------
User1                                  Yes
User2                                  Yes
```

- **show acl detailed** <ACL_Name>: visualizza informazioni dettagliate sugli ACL configurati.Di

seguito è riportato un esempio:**Nota:** alcune delle linee nell'output sono state spostate nella seconda linea a causa dei vincoli di spazio.

```
Cisco Controller) >show acl detailed User1

                    Source                          Destination
   Source Port   Dest Port
I  Dir        IP Address/Netmask               IP Address/Netmask
   Prot     Range        Range     DSCP    Action
-- --- ------------------------------- -------------------------------
   ---- ----------- ----------- ----     ------
 1  In       172.16.0.0/255.255.0.0         172.16.1.100/255.255.255.255
   Any   0-65535        0-65535    Any     Permit
 2 Out     172.16.1.100/255.255.255.255       172.16.0.0/255.255.0.0
   Any   0-65535        0-65535    Any     Permit


(Cisco Controller) >show acl detailed User2

                    Source                          Destination
   Source Port   Dest Port
I  Dir        IP Address/Netmask               IP Address/Netmask
   Prot     Range        Range     DSCP Action
-- --- ------------------------------- -------------------------------
   ---- ----------- ----------- ---- ------
1  In       172.16.0.0/255.255.0.0          172.16.1.50/255.255.255.255
   Any    0-65535        0-65535     Any   Permit
2 Out      172.16.1.50/255.255.255.255       172.16.0.0/255.255.0.0
   Any    0-65535        0-65535     Any   Permit
```

- **show client detail** <Indirizzo MAC del client> - Visualizza informazioni dettagliate sul client wireless.

Suggerimenti per la risoluzione dei problemi

Suggerimenti per la risoluzione dei problemi:

- Verificare sul controller che il server RADIUS sia in stato attivo e non in standby o disabilitato.
- Sul controller, verificare se il server RADIUS è stato scelto dal menu a discesa della rete WLAN (SSID).
- 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.

Informazioni correlate

- ACL sui controller LAN wireless: Regole, limitazioni ed esempi
- Esempio di configurazione degli ACL sui controller LAN wireless
- Esempio di configurazione di filtri MAC con controller WLC
- Guida alla configurazione di Cisco Wireless LAN Controller, versione 5.2
- Documentazione e supporto tecnico – Cisco Systems