Configurazione di un server RADIUS e di un WLC per l'assegnazione dinamica della VLAN

Sommario

Introduzione

In questo documento viene spiegato il concetto di assegnazione dinamica delle VLAN. In questo documento viene descritto come configurare il controller WLC (Wireless LAN Controller) e un server RADIUS per assegnare dinamicamente i client WLAN (Wireless LAN) a una VLAN specifica.

Prerequisiti

Requisiti

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

- Conoscere a fondo i WLC e i Lightweight Access Point (LAP)
- Conoscenza funzionale del server AAA
- Conoscere a fondo le reti wireless e i problemi di sicurezza wireless

- Conoscenze base di LWAPP (Lightweight AP Protocol)

Componenti usati

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

- Cisco 4400 WLC con firmware release 5.2
- Cisco serie 1130 LAP
- Cisco 802.11a/b/g Wireless Client Adapter con firmware versione 4.4
- Cisco Aironet Desktop Utility (ADU) con versione 4.4
- Cisco Secure Access Control Server (ACS) con versione 4.1
- Cisco serie 2950 switch

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.

Assegnazione dinamica di VLAN con server RADIUS

Nella maggior parte dei sistemi WLAN, ogni WLAN dispone di un criterio statico che viene applicato a tutti i client associati a un SSID (Service Set Identifier) o a una WLAN nella terminologia del controller. Sebbene potente, questo metodo presenta delle limitazioni in quanto richiede ai client di associarsi a SSID diversi per ereditare criteri QoS e di sicurezza diversi.

Tuttavia, la soluzione Cisco WLAN supporta le reti di identità. Ciò consente alla rete di annunciare un singolo SSID, ma consente a utenti specifici di ereditare criteri QoS o di sicurezza diversi in base alle credenziali utente.

L'assegnazione dinamica della VLAN è una di queste funzionalità che permette a un utente wireless di accedere a una VLAN specifica in base alle credenziali fornite dall'utente. L'assegnazione degli utenti a una VLAN specifica viene gestita da un server di autenticazione RADIUS, ad esempio CiscoSecure ACS. Questa funzione può essere utilizzata, ad esempio, per fare in modo che l'host wireless rimanga sulla stessa VLAN su cui si sposta all'interno della rete di un campus.

Pertanto, quando un client tenta di associarsi a un LAP registrato con un controller, il LAP passa le credenziali dell'utente al server RADIUS per la convalida. Una volta completata l'autenticazione, il server RADIUS passa all'utente alcuni attributi IETF (Internet Engineering Task Force). Questi attributi RADIUS determinano l'ID VLAN da assegnare al client wireless. L'SSID (WLAN, in termini di WLC) del client non conta perché l'utente è sempre assegnato a questo ID VLAN predeterminato.

Gli attributi utente RADIUS utilizzati per l'assegnazione dell'ID VLAN sono:

- IETF 64 (Tipo tunnel) - Impostare questa opzione su VLAN.
- IETF 65 (Tunnel Medium Type) - Impostato su 802
- IETF 81 (Tunnel Private Group ID) - Imposta su VLAN ID.

L'ID VLAN è a 12 bit e accetta un valore compreso tra 1 e 4094 inclusi. Poiché Tunnel-Private-Group-ID è di tipo stringa, come definito nella RFC2868 per l'utilizzo con IEEE 802.1X, il valore intero dell'ID VLAN viene codificato come stringa. Quando vengono inviati questi attributi del tunnel, è necessario compilare il campo Tag.

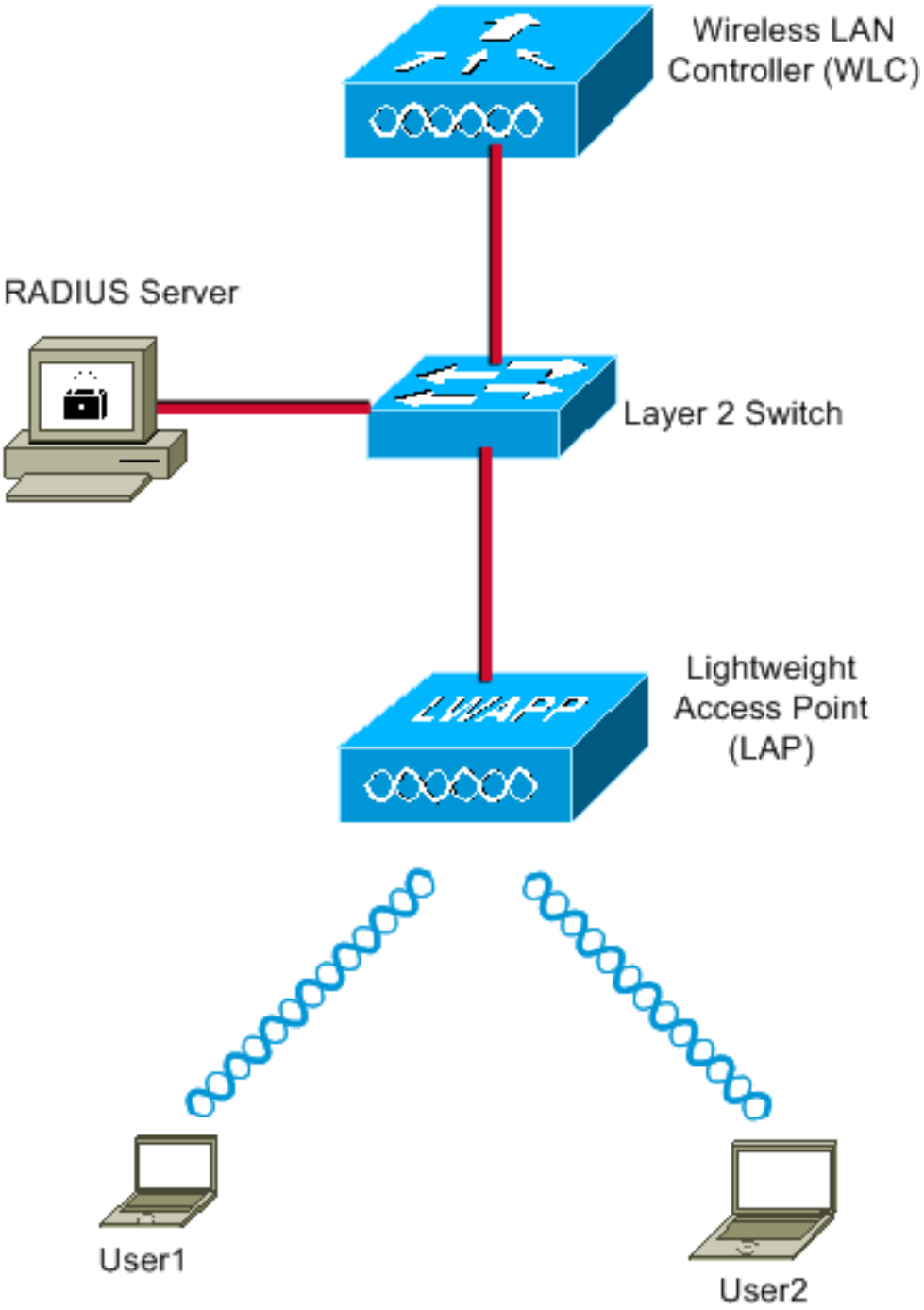
Come indicato nella RFC2868 , sezione 3.1: **Il campo Tag è lungo un ottetto e serve a raggruppare gli attributi dello stesso pacchetto che fanno riferimento allo stesso tunnel.** I valori validi per questo campo sono compresi tra 0x01 e 0x1F inclusi. Se il campo Tag non è utilizzato, deve essere zero (0x00). Per ulteriori informazioni su tutti gli attributi RADIUS, consultare la RFC 2868 .

Configurazione

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

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Di seguito sono riportati i dettagli di configurazione dei componenti utilizzati nel diagramma:

- L'indirizzo IP del server ACS (RADIUS) è 172.16.1.1.
- L'indirizzo dell'interfaccia di gestione del WLC è 172.16.1.30.
- L'indirizzo dell'interfaccia AP-Manager del WLC è 172.16.1.31.
- L'indirizzo del server DHCP 172.16.1.1 viene usato per assegnare gli indirizzi IP al protocollo LWAPP. **Il server DHCP interno sul controller viene utilizzato per assegnare l'indirizzo IP ai client wireless.**
- VLAN10 e VLAN11 vengono usate in questa configurazione. L'utente 1 è configurato per essere inserito nella VLAN10 e l'utente 2 è configurato per essere inserito nella VLAN11 dal server RADIUS.**Nota:** questo documento mostra solo tutte le informazioni di configurazione relative a user1. Completare la stessa procedura descritta in questo documento per user2.
- Questo documento utilizza 802.1x con LEAP come meccanismo di sicurezza.**Nota:** Cisco consiglia di utilizzare metodi di autenticazione avanzati, come l'autenticazione EAP-FAST e EAP-TLS, per proteggere la WLAN. Questo documento utilizza LEAP solo per semplicità.

Configurazione

Prima della configurazione, per questo documento si presume che il LAP sia già stato registrato sul WLC. Per ulteriori informazioni, fare riferimento agli esempi di configurazione base di Wireless LAN Controller e Lightweight Access Point. Per informazioni sulla procedura di registrazione utilizzata, consultare il documento sulla registrazione di un Lightweight AP (LAP) su un Wireless LAN Controller (WLC).

Procedura di configurazione

Questa configurazione è suddivisa in tre categorie:

1. Configurazione server RADIUS
2. Configurazione dello switch per più VLAN
3. Configurazione WLC
4. Configurazione Wireless Client Utility

Configurazione server RADIUS

Questa configurazione richiede i seguenti passaggi:

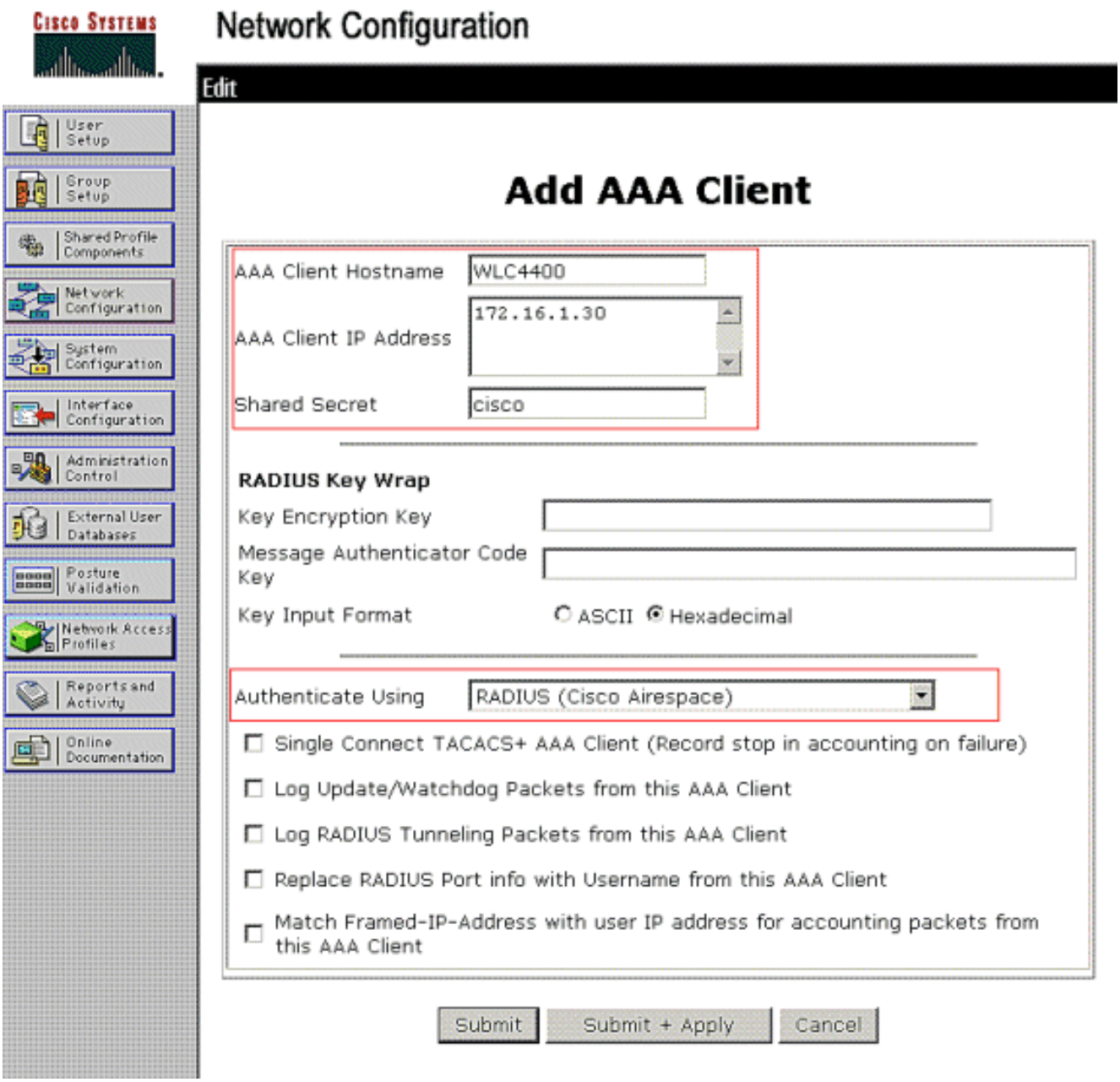
- Configurare il WLC come client AAA sul server RADIUS
- Configurare gli utenti e gli attributi RADIUS (IETF) utilizzati per l'assegnazione dinamica della VLAN sul server RADIUS

Configurare il client AAA per il WLC sul server RADIUS

In questa procedura viene illustrato come aggiungere il WLC come client AAA sul server RADIUS in modo che il WLC possa passare le credenziali utente al server RADIUS.

Attenersi alla seguente procedura:

1. Dalla GUI di ACS, fare clic su **Network Configuration** (Configurazione di rete).
2. Fare clic sulla sezione **Add Entry** (Aggiungi voce) nel campo Client AAA.
3. Immettere l'indirizzo IP e la chiave del client AAA.L'indirizzo IP deve essere l'indirizzo IP dell'interfaccia di gestione del WLC.Accertarsi che la chiave immessa sia la stessa configurata sul WLC nella finestra Security. Chiave segreta utilizzata per la comunicazione tra il client AAA (WLC) e il server RADIUS.
4. Selezionare **RADIUS (Cisco Airespace)** dal campo Autentica con per il tipo di autenticazione.

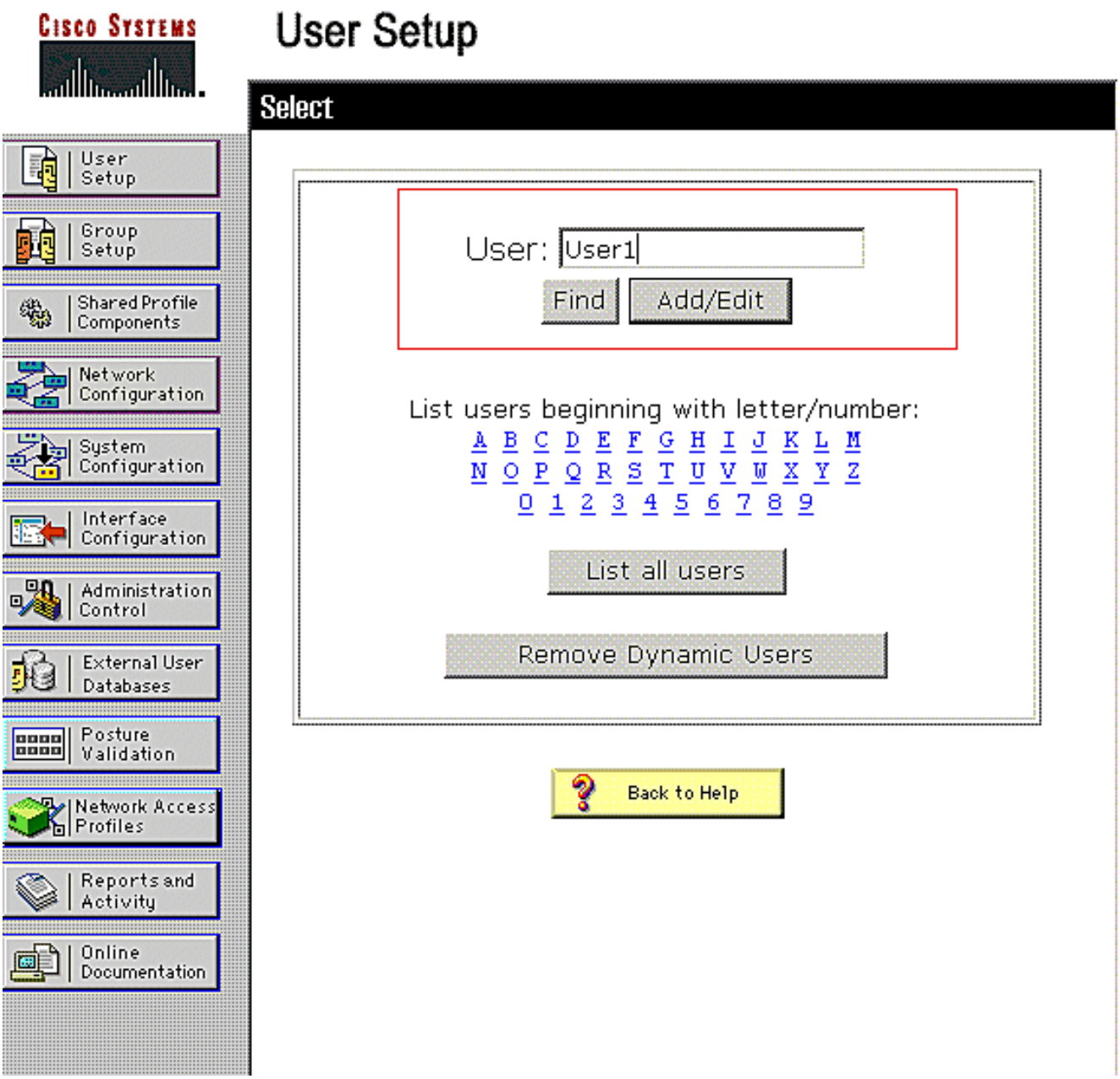


Configurare gli utenti e gli attributi RADIUS (IETF) utilizzati per l'assegnazione dinamica della VLAN sul server RADIUS

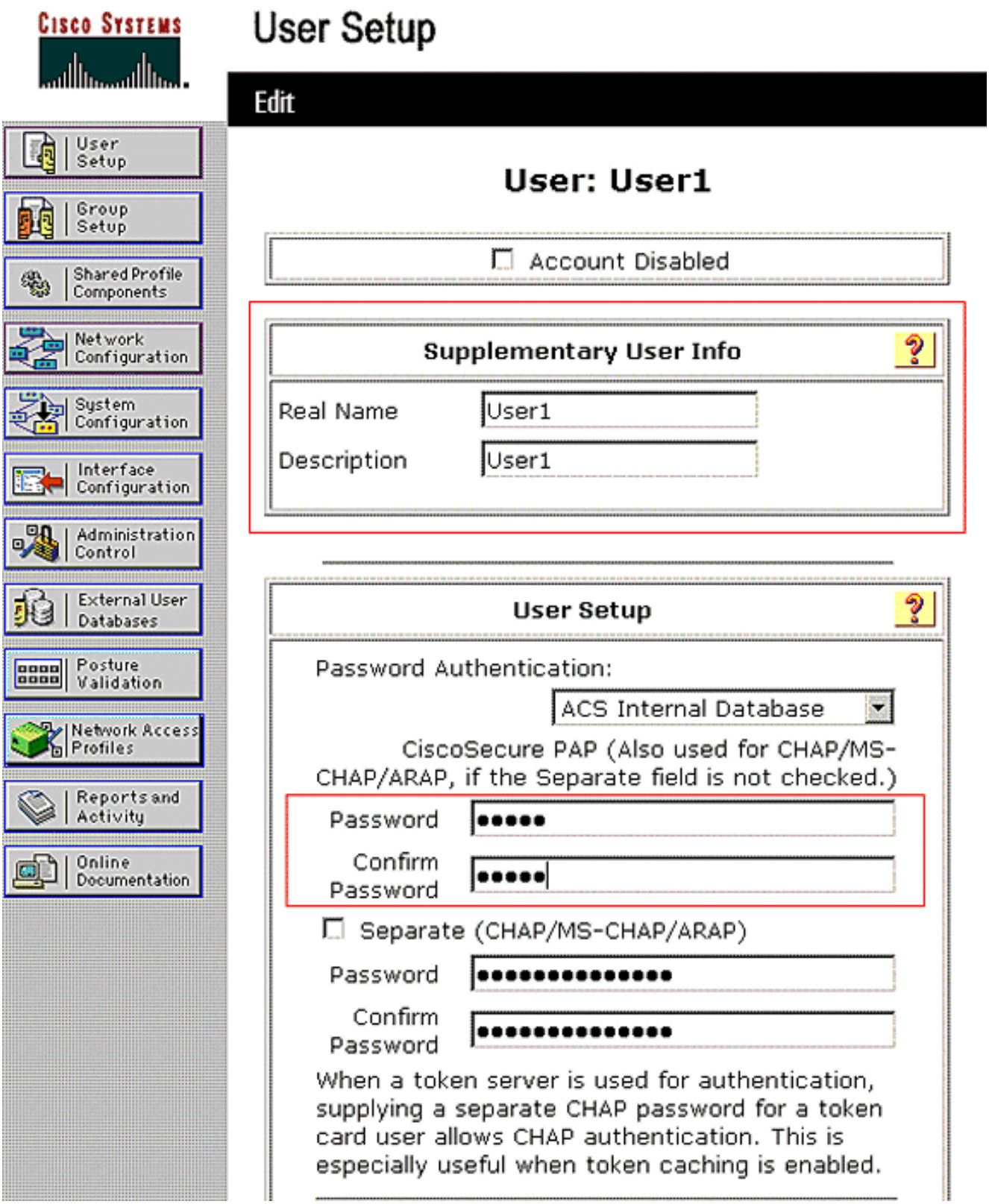
In questa procedura viene illustrato come configurare gli utenti nel server RADIUS e gli attributi RADIUS (IETF) utilizzati per assegnare gli ID VLAN a tali utenti.

Attenersi alla seguente procedura:

1. Dalla GUI di ACS, fare clic su **User Setup** (Configurazione utente).
2. Nella finestra Impostazione utente, immettere un nome utente nel campo Utente e fare clic su
Aggiungi/Modifica.

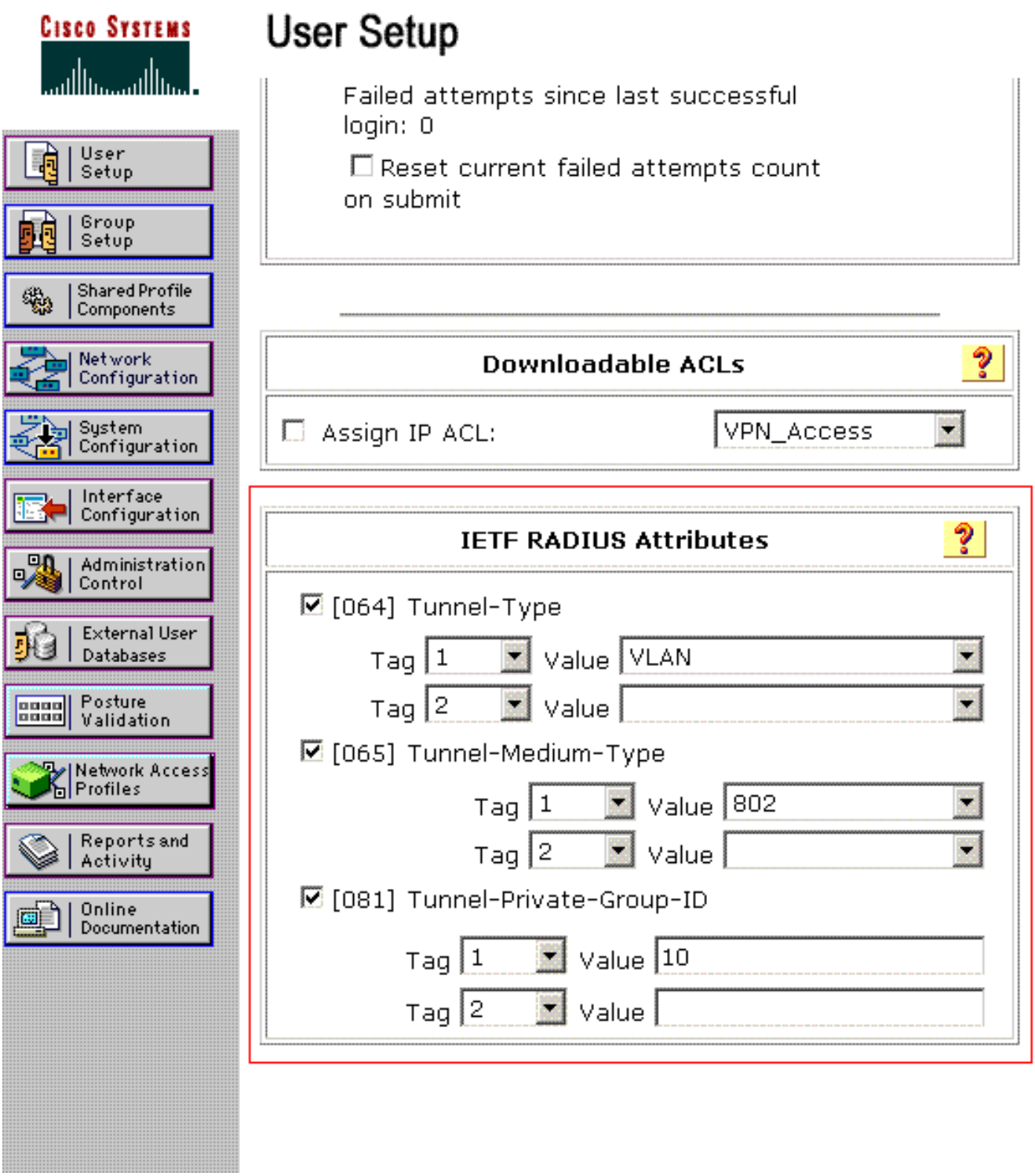


3. Nella pagina Modifica immettere le informazioni utente necessarie, come illustrato di seguito:

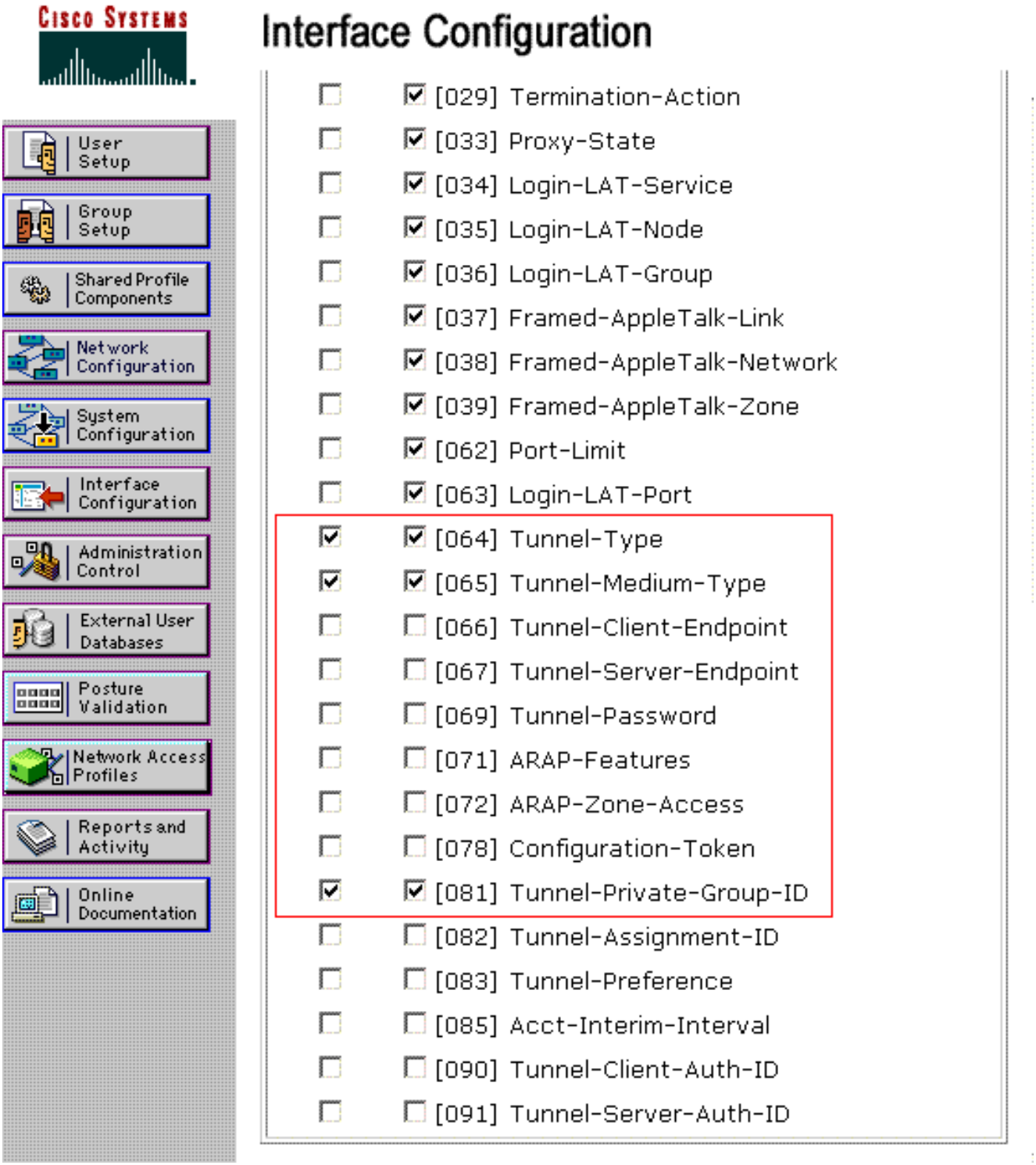


In questo diagramma, si noti che la password fornita nella sezione Impostazione utente deve essere la stessa fornita sul lato client durante l'autenticazione dell'utente.

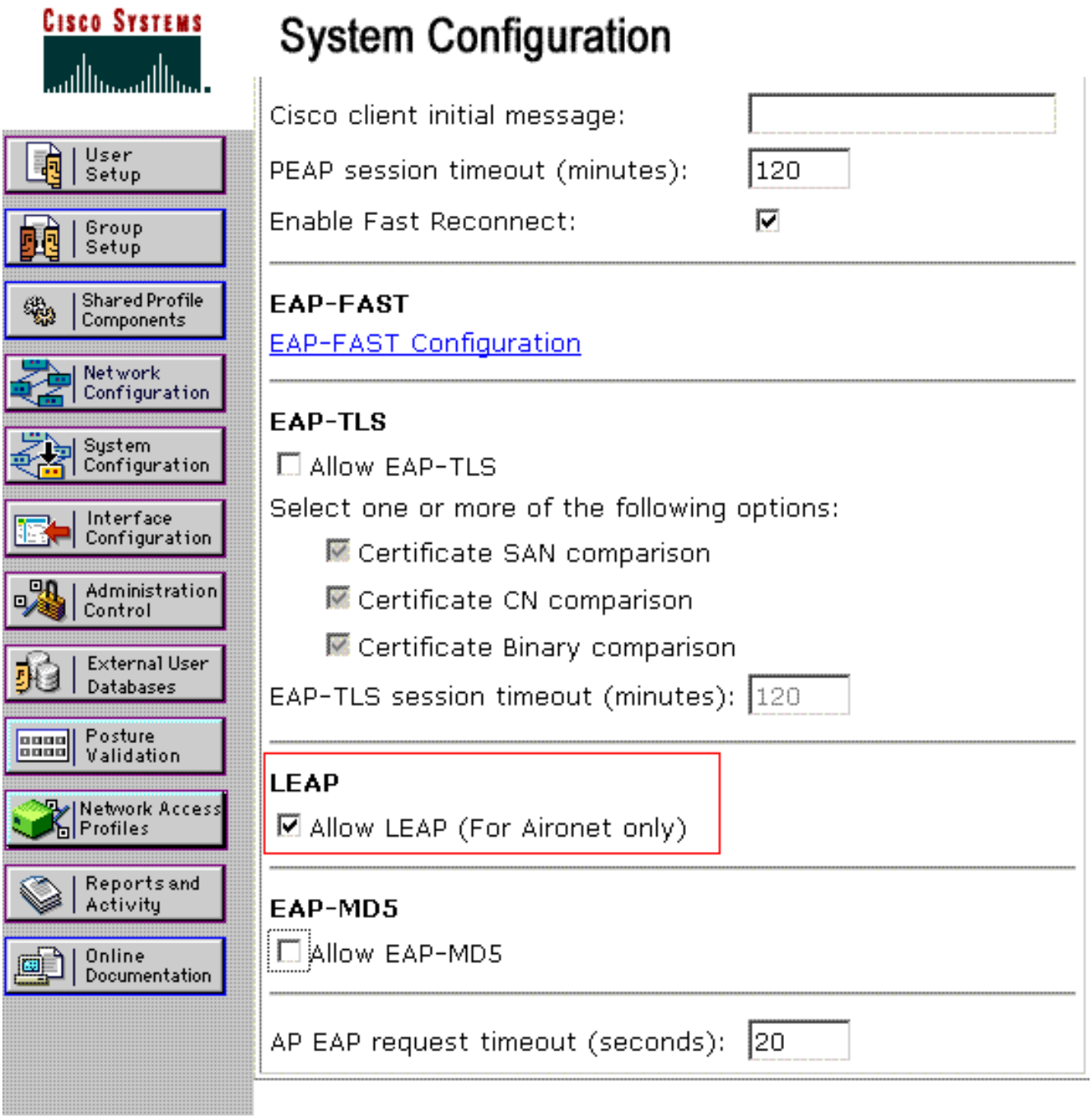
4. Scorrere la pagina Modifica e individuare il campo **Attributi RADIUS IETF**.
5. Nel campo Attributi RADIUS IETF, selezionare le caselle di controllo accanto ai tre attributi Tunnel e configurare i valori degli attributi come mostrato di seguito:



Nota: nella configurazione iniziale del server ACS, gli attributi RADIUS IETF potrebbero non essere visualizzati.Per abilitare gli attributi IETF nella finestra di configurazione utente, scegliere **Configurazione interfaccia > RADIUS (IETF)**.Selezionare quindi le caselle di controllo relative agli attributi **64, 65 e 81** nelle colonne Utente e Gruppo.



Nota: affinché il server RADIUS assegni dinamicamente il client a una VLAN specifica, **è necessario che l'ID VLAN configurato nel campo IETF 81 (Tunnel-Private-Group-ID) del server RADIUS sia presente sul WLC.**Selezionare la casella di controllo dell'attributo **Per Utente TACACS+/RADIUS** in Configurazione interfaccia > Opzioni avanzate per abilitare il server RADIUS per le configurazioni per utente.Inoltre, poiché il protocollo LEAP viene utilizzato come protocollo di autenticazione, assicurarsi che sia abilitato nella finestra Configurazione di sistema del server RADIUS, come mostrato di seguito:



Configurazione dell'ACS con gli attributi VSA di Cisco Airespace per l'assegnazione dinamica della VLAN

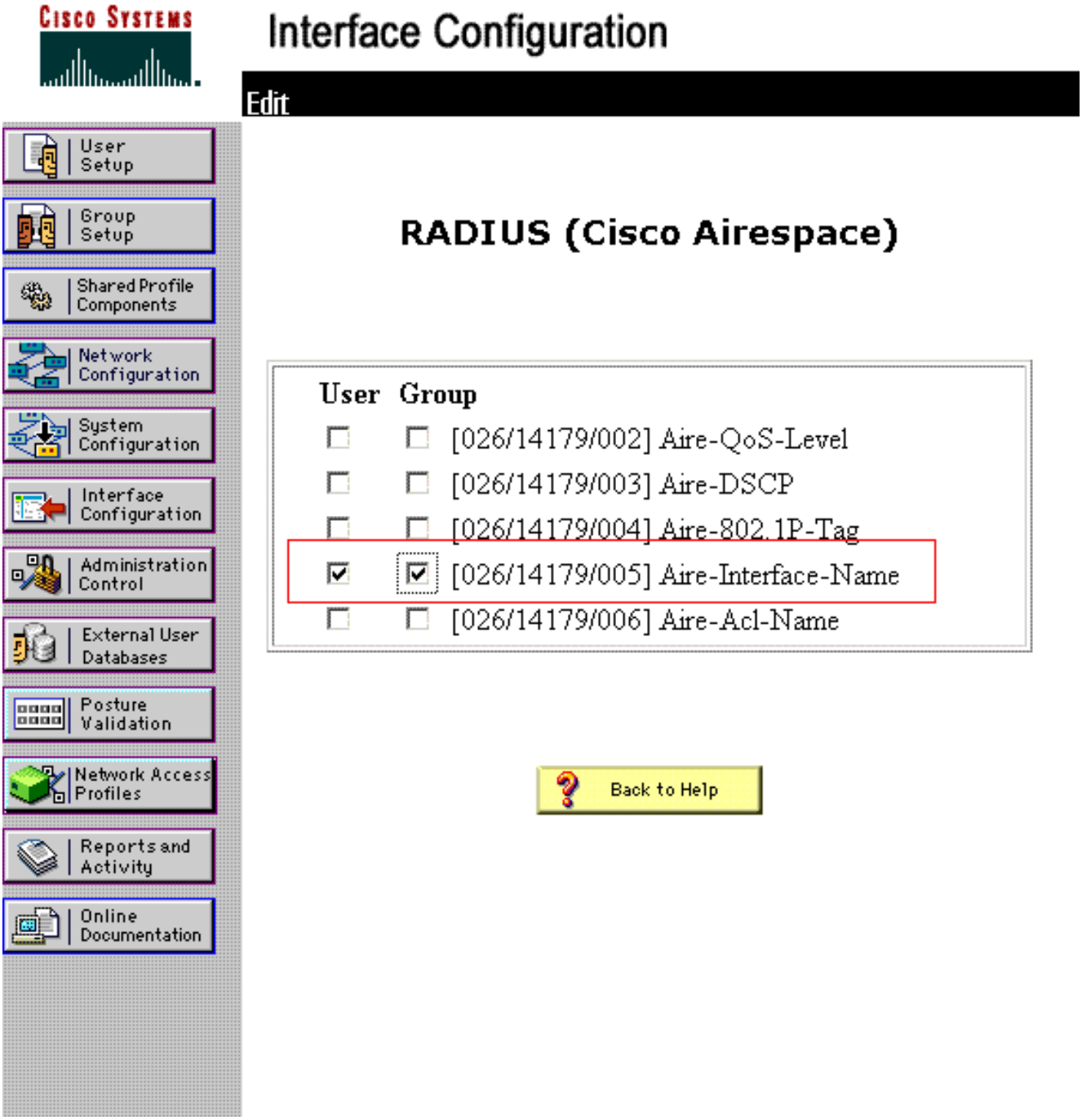
Nelle versioni più recenti di ACS, è possibile anche configurare l'attributo Cisco Airespace [VSA (specifico del fornitore)] per assegnare a un utente autenticato con un nome di interfaccia VLAN (non l'ID VLAN), in base alla configurazione utente su ACS. A tale scopo, eseguire la procedura descritta in questa sezione.

Nota: in questa sezione viene usata la versione ACS 4.1 per configurare l'attributo VSA di Cisco Airespace.

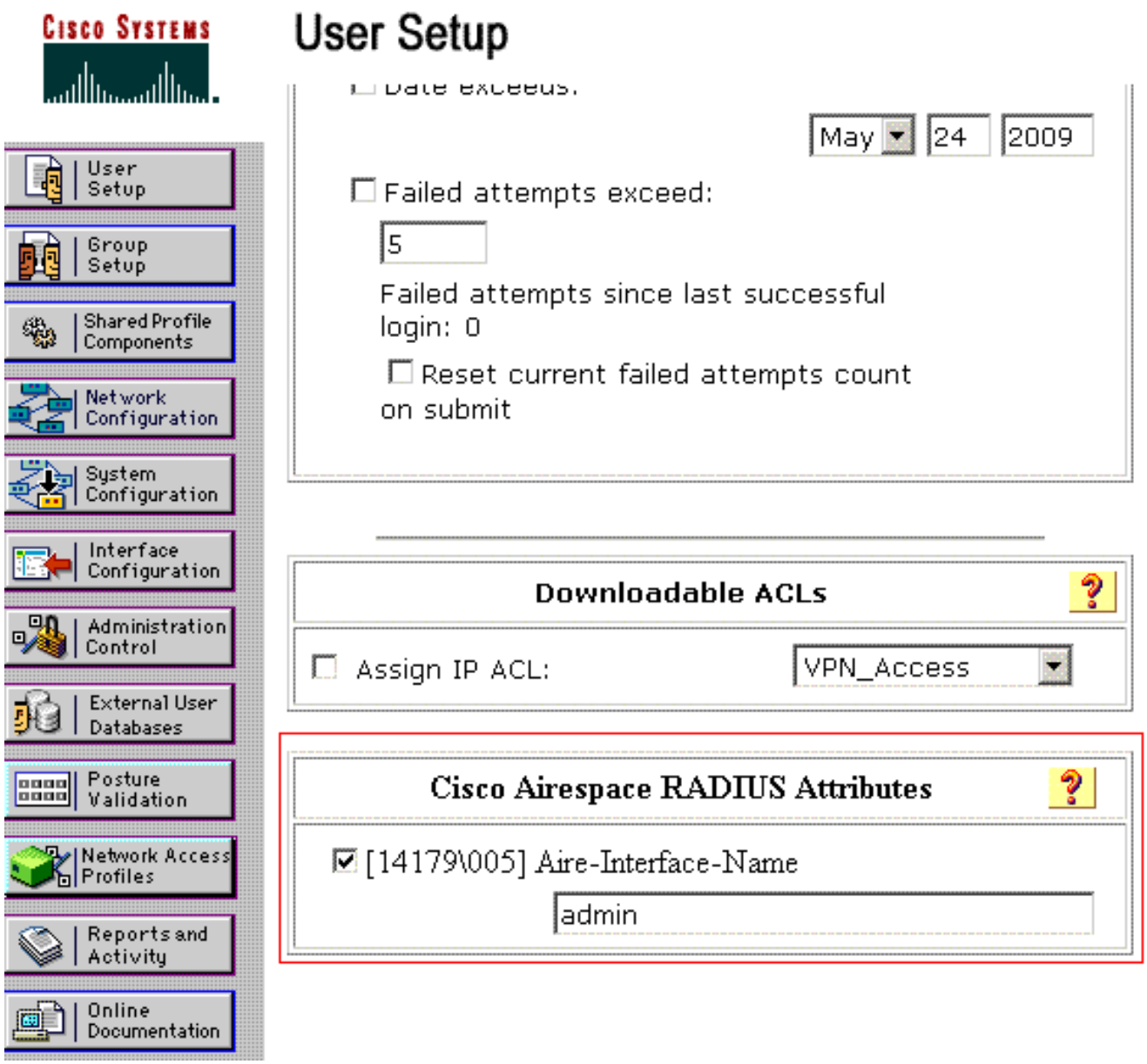
Configurazione del gruppo ACS con l'opzione Cisco Airespace VSA Attribute

Attenersi alla seguente procedura:

1. Dalla GUI di ACS 4.1, fare clic su **Interface Configuration** (Configurazione interfaccia) dalla barra di navigazione. Quindi, selezionare **RADIUS (Cisco Airespace)** dalla pagina Configurazione interfaccia per configurare l'opzione dell'attributo Cisco Airespace.
2. Dalla finestra RADIUS (Cisco Airespace), selezionare la casella di controllo Utente (se necessario, la casella di controllo Gruppo) accanto a **Aire-Interface-Name** per visualizzarla nella pagina User Edit. Fare quindi clic su **Invia**.



3. Andare alla pagina Modifica dell'utente 1.
4. Dalla pagina User Edit, scorrere verso il basso fino alla sezione **Cisco Airespace RADIUS Attributes**. Selezionare la casella di controllo accanto all'attributo **Aire-Interface-Name** e specificare il nome dell'interfaccia dinamica da assegnare al completamento dell'autenticazione utente.In questo esempio viene assegnata alla VLAN **di amministrazione**.



5. Fare clic su **Invia**.

Configurazione dello switch per più VLAN

Per consentire l'uso di più VLAN sullo switch, è necessario usare questi comandi per configurare la porta dello switch connessa al controller:

1. Switch(config-if)#**switchport mode trunk**
2. Switch(config-if)#**switchport trunk encapsulation dot1q**

Nota: per impostazione predefinita, la maggior parte degli switch consente tutte le VLAN create sullo switch tramite la porta trunk.

Questi comandi variano per uno switch Catalyst con sistema operativo (CatOS).

Se allo switch è collegata una rete cablata, è possibile applicare la stessa configurazione alla porta dello switch che si connette alla rete cablata. Ciò consente la comunicazione tra le stesse VLAN nella rete cablata e wireless.

Nota: in questo documento non viene descritta la comunicazione tra VLAN. Questo aspetto esula tuttavia dalle finalità del presente documento. Per il routing tra VLAN, è necessario usare uno

switch di layer 3 o un router esterno con configurazioni VLAN e trunking appropriate. La configurazione del routing tra VLAN è spiegata in diversi documenti.

Configurazione WLC

Questa configurazione richiede i seguenti passaggi:

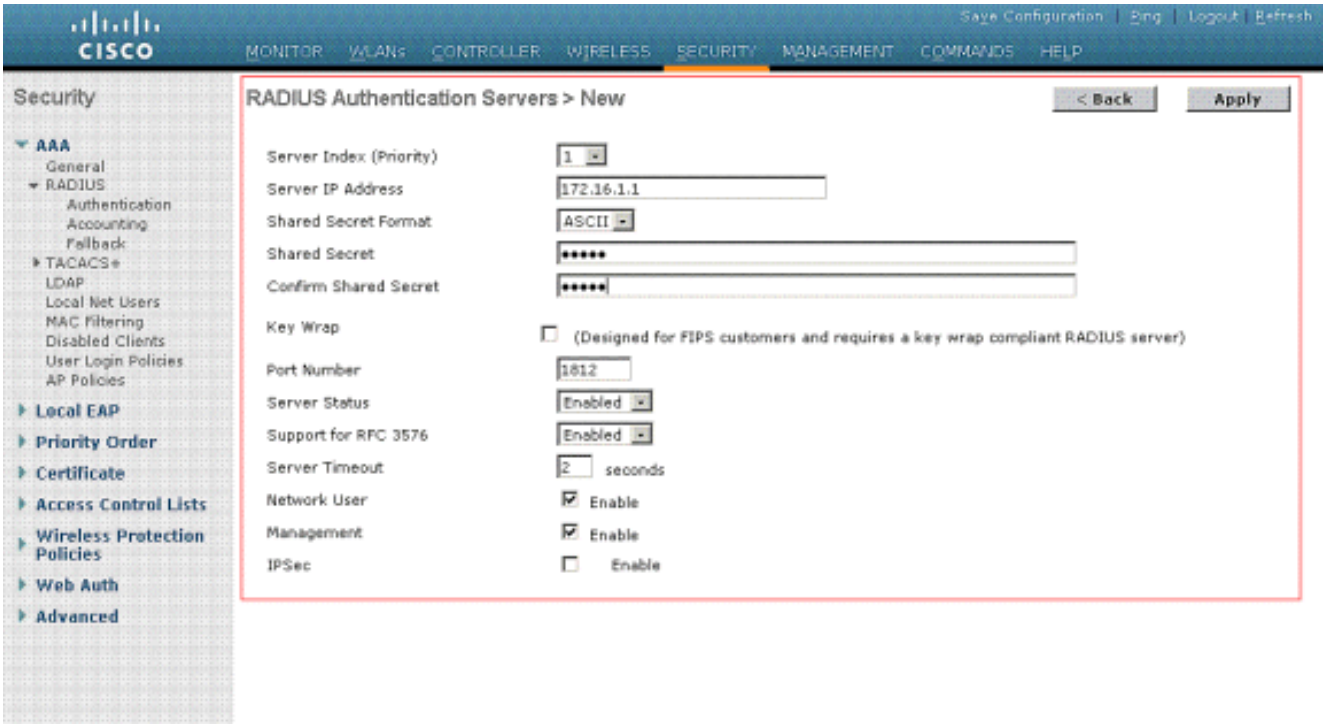
- Configurare il WLC con i dettagli del server di autenticazione
- Configurazione delle interfacce dinamiche (VLAN)
- Configurazione delle WLAN (SSID)

Configurare il WLC con i dettagli del server di autenticazione

Ènecessario configurare il WLC in modo che possa comunicare con il server RADIUS per autenticare i client e anche per qualsiasi altra transazione.

Attenersi alla seguente procedura:

1. Dalla GUI del controller, fare clic su **Security** (Sicurezza).
2. Immettere l'indirizzo IP del server RADIUS e la chiave privata condivisa utilizzata tra il server RADIUS e il WLC.La chiave privata condivisa deve essere la stessa configurata nel server RADIUS in Configurazione di rete > Client AAA > Aggiungi voce. Di seguito è riportato un esempio di finestra del
WLC:



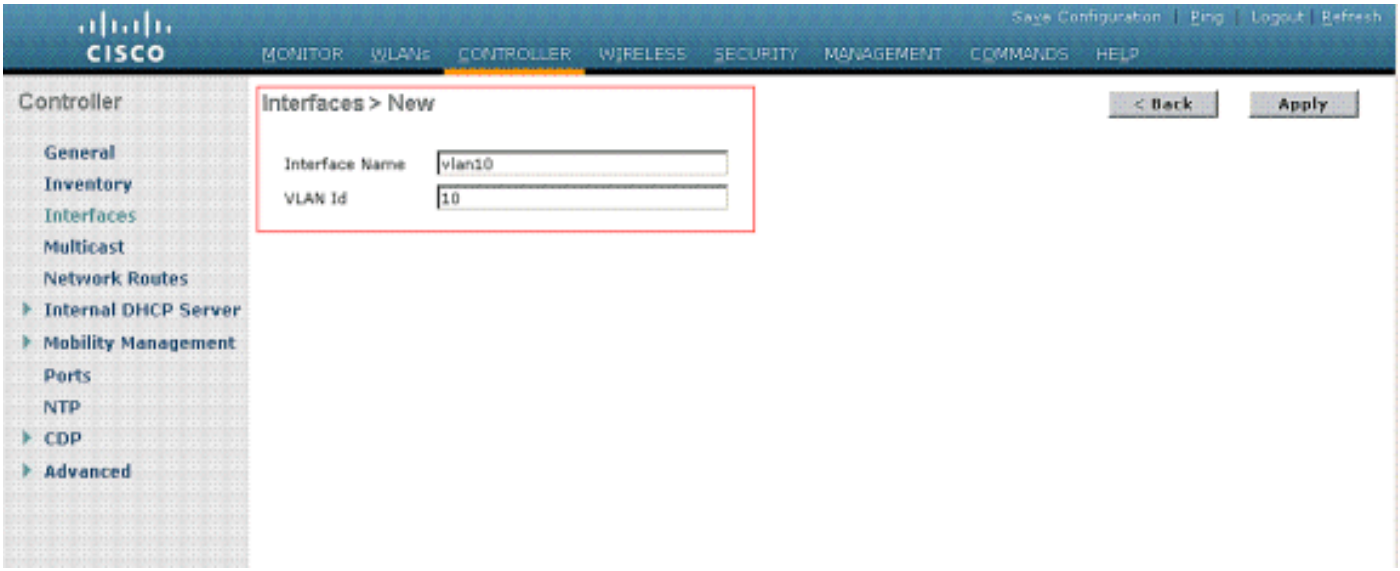
Configurazione delle interfacce dinamiche (VLAN)

In questa procedura viene spiegato come configurare le interfacce dinamiche sul WLC. Come spiegato in precedenza in questo documento, l'ID VLAN specificato nell'attributo Tunnel-Private-Group ID del server RADIUS deve esistere anche nel WLC.

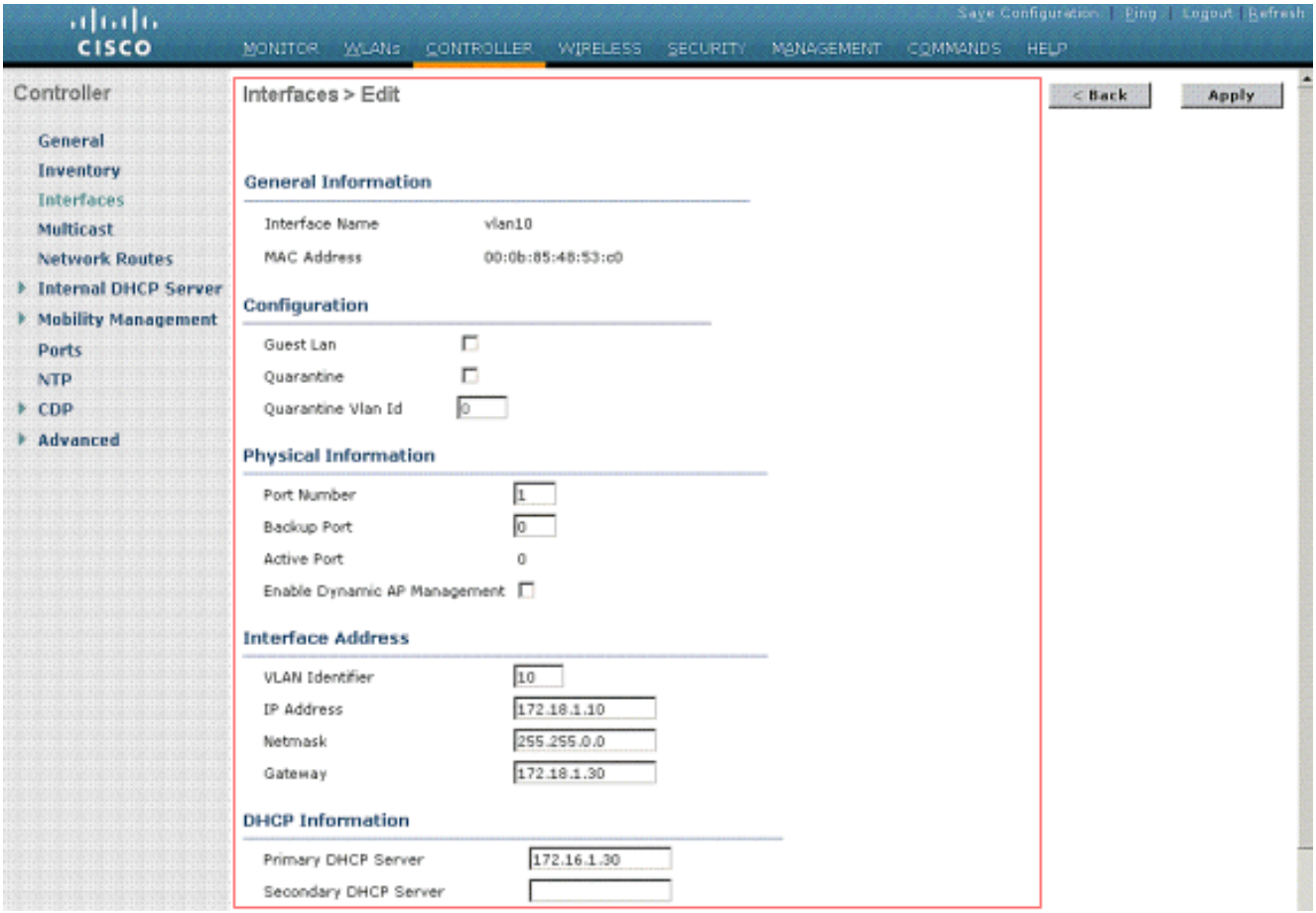
Nell'esempio, l'utente 1 viene specificato con l'**ID tunnel-gruppo privato di 10 (VLAN =10)** sul

server RADIUS. Vedere la sezione Attributi RADIUS IETF della finestra Impostazione utente 1.

In questo esempio, è possibile vedere la stessa interfaccia dinamica (VLAN=10) configurata nel WLC. Dalla GUI del controller, nella finestra Controller > Interfacce, viene configurata l'interfaccia dinamica.



1. Fare clic su **Apply** (Applica) in questa finestra.Viene visualizzata la finestra Edit (Modifica) di questa interfaccia dinamica (qui VLAN 10).
2. Immettere l'indirizzo IP e il gateway predefinito dell'interfaccia dinamica.



Nota: poiché in questo documento viene usato un server DHCP interno sul controller, il campo del server DHCP primario di questa finestra punta all'interfaccia di gestione del WLC stesso. Ai client wireless è inoltre possibile utilizzare un server DHCP esterno, un router o lo

stesso server RADIUS come server DHCP. In questi casi, il campo del server DHCP primario punta all'indirizzo IP del dispositivo utilizzato come server DHCP. Per ulteriori informazioni, consultare la documentazione del server DHCP in uso.

3. Fare clic su **Apply** (Applica).A questo punto, si è configurati con un'interfaccia dinamica nel WLC. Analogamente, è possibile configurare diverse interfacce dinamiche nel WLC. Tuttavia, tenere presente che lo stesso ID VLAN deve essere presente anche nel server RADIUS perché la VLAN specifica possa essere assegnata al client.

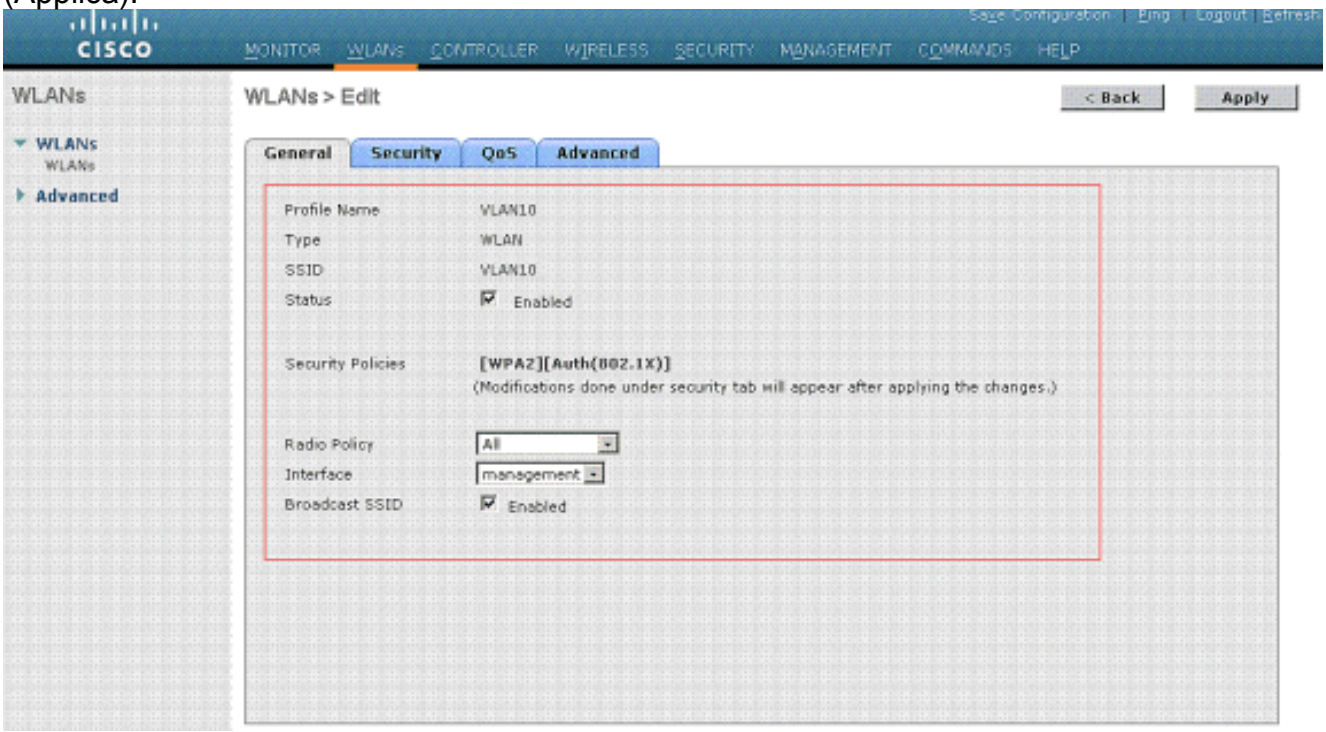
Configurazione delle WLAN (SSID)

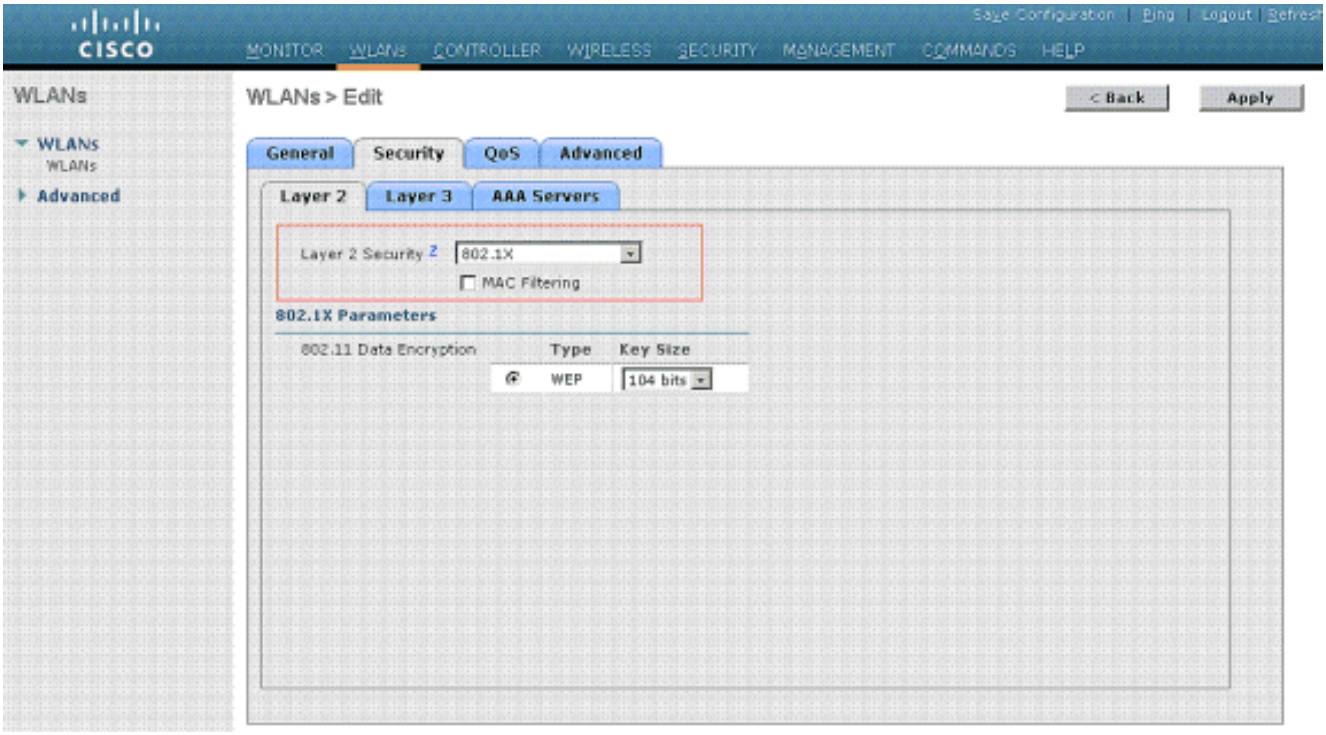
In questa procedura viene spiegato come configurare le WLAN nel WLC.

Attenersi alla seguente procedura:

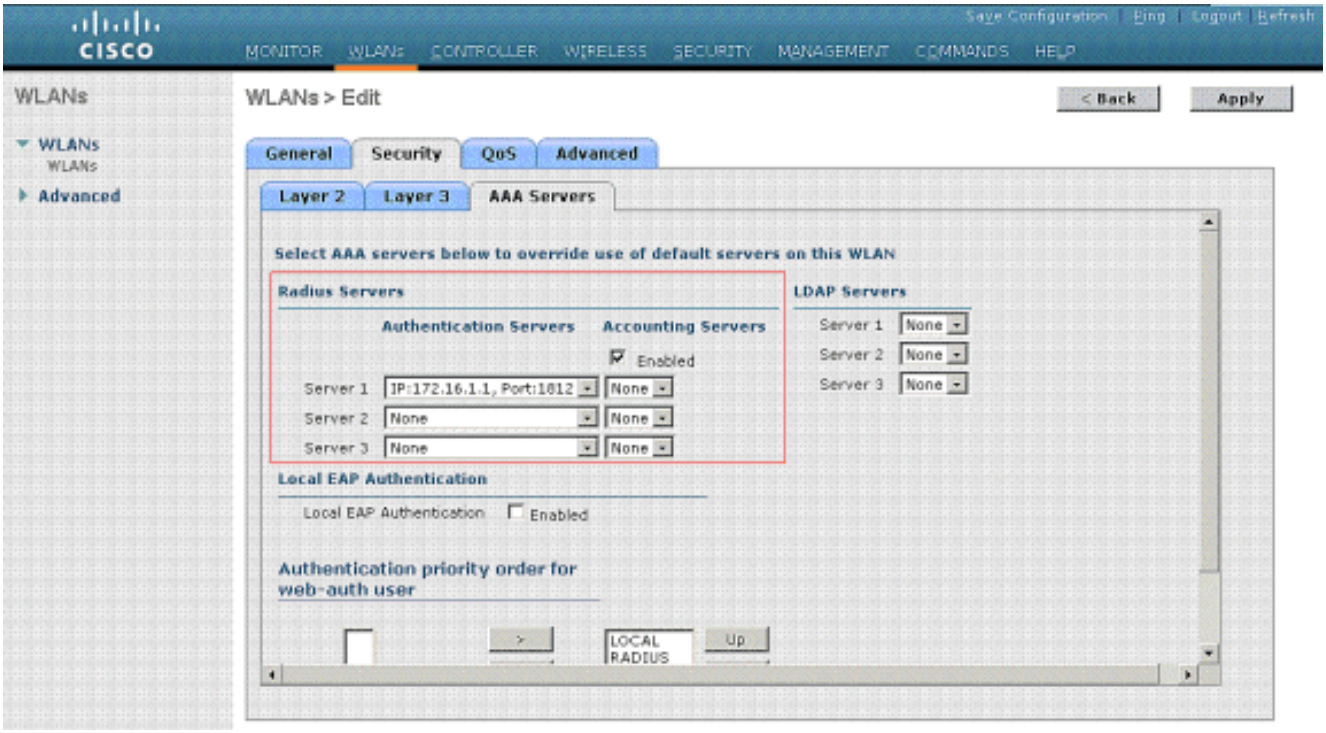
1. Dalla GUI del controller, selezionare **WLAN > New** (Nuova) per creare una nuova WLAN.Viene visualizzata la finestra Nuove WLAN.
2. Immettere l'ID WLAN e le informazioni sull'SSID WLAN.Èpossibile immettere qualsiasi nome come SSID WLAN. In questo esempio viene usato VLAN10 come SSID WLAN.

3. Per accedere alla finestra Modifica di WLAN SSID10, fare clic su **Apply** (Applica).





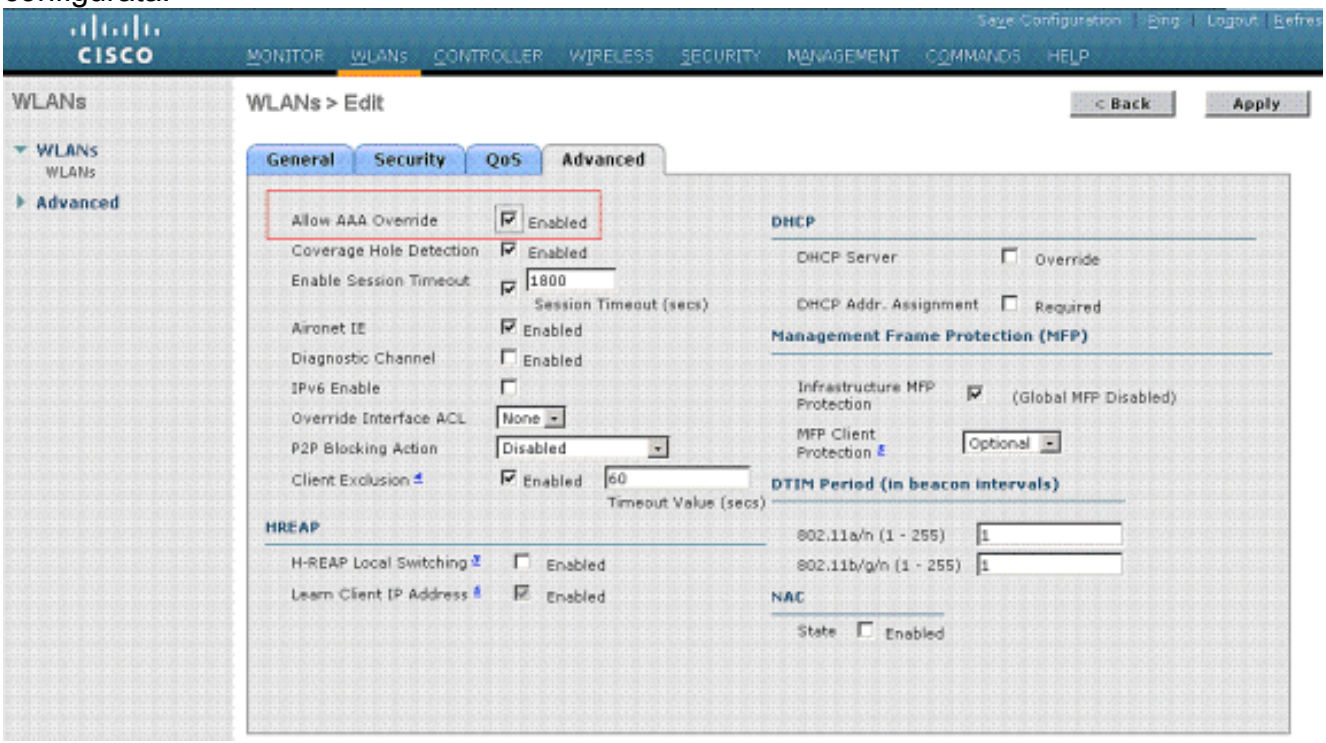
In genere, in un controller LAN wireless, a ciascuna WLAN viene eseguito il mapping a una VLAN (SSID) specifica in modo che un utente specifico appartenente alla WLAN venga inserito nella VLAN mappata. Questa mappatura viene in genere eseguita nel campo Interface Name (Nome interfaccia) della finestra SSID della WLAN.



Nell'esempio riportato, è compito del server RADIUS assegnare un client wireless a una VLAN specifica dopo la riuscita dell'autenticazione. Non è necessario mappare le WLAN a un'interfaccia dinamica specifica sul WLC. Oppure, anche se il mapping tra la WLAN e l'interfaccia dinamica viene eseguito sul WLC, il server RADIUS ignora questo mapping e assegna l'utente che passa attraverso la WLAN alla VLAN specificata nel campo user **Tunnel-Group-Private-ID** nel server RADIUS.

4. Selezionare la casella di controllo **Consenti sostituzione AAA** per sostituire le configurazioni WLC con il server RADIUS.

5. Abilitare l'opzione Allow AAA Override nel controller per ciascuna WLAN (SSID) configurata.



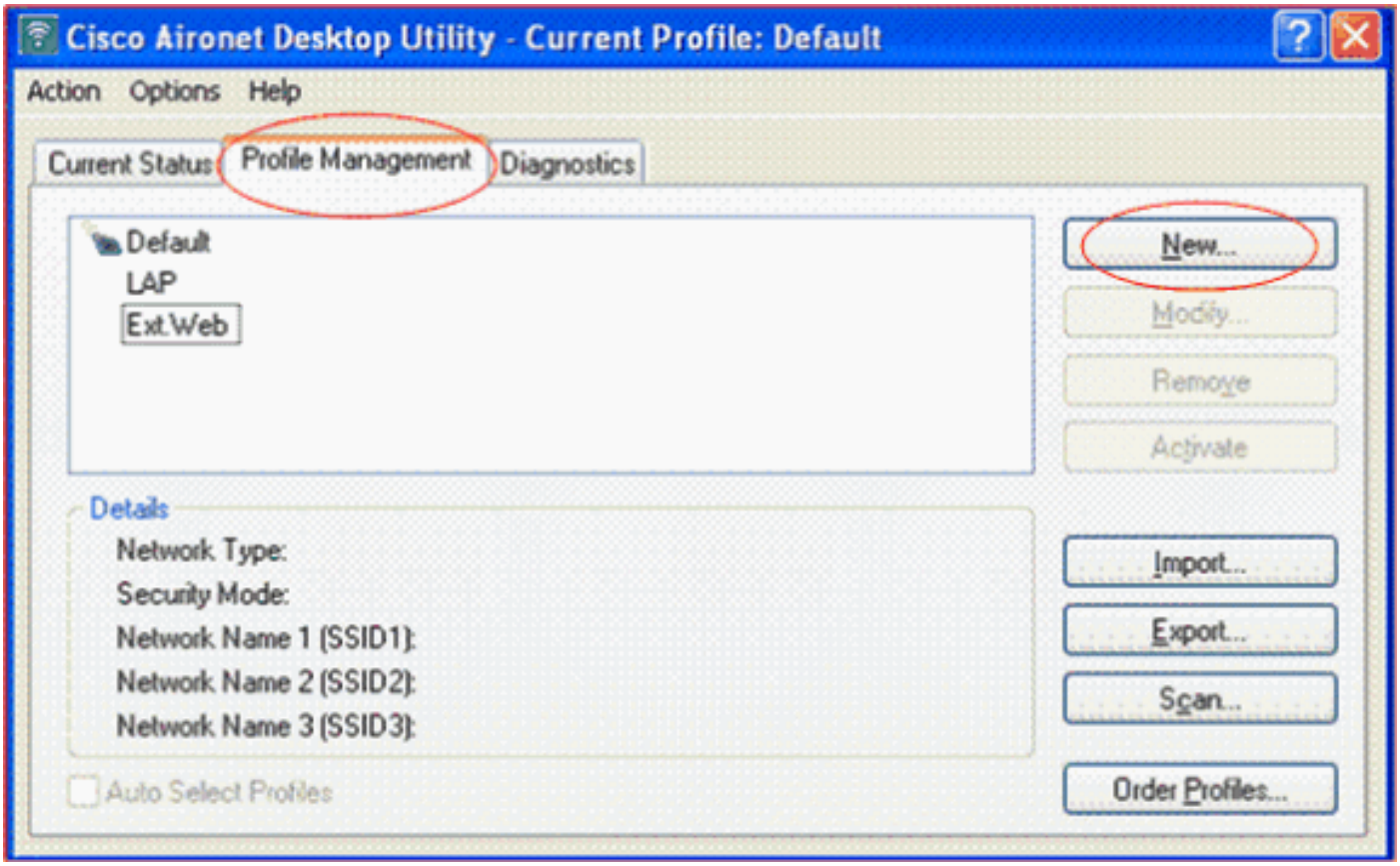
Quando l'override AAA è abilitato e un client ha parametri di autenticazione WLAN AAA e controller in conflitto, l'autenticazione del client viene eseguita dal server AAA (RADIUS). Come parte di questa autenticazione, il sistema operativo sposta i client su una VLAN restituita dal server AAA. Questa impostazione è predefinita nella configurazione dell'interfaccia del controller.Ad esempio, se la WLAN aziendale utilizza principalmente un'interfaccia di gestione assegnata alla VLAN 2 e l'override AAA restituisce un reindirizzamento alla VLAN 100, il sistema operativo reindirizza tutte le trasmissioni client alla VLAN 100 anche se la porta fisica a cui è assegnata la VLAN 100. Quando l'override AAA è disabilitato, tutte le impostazioni predefinite di autenticazione del client corrispondono alle impostazioni dei parametri di autenticazione del controller e l'autenticazione viene eseguita dal server AAA solo se la WLAN del controller non contiene parametri di autenticazione specifici del client.

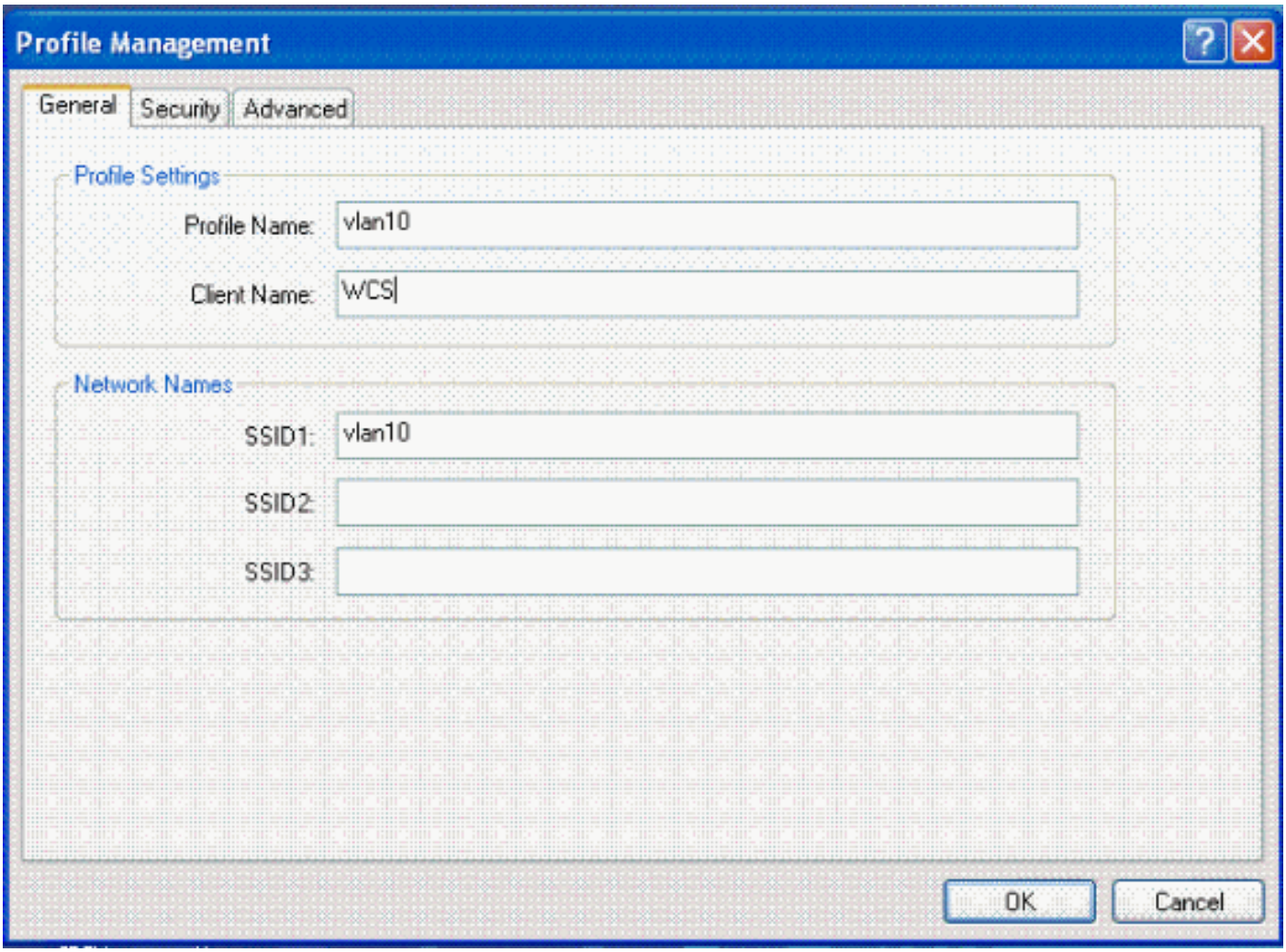
Configurazione Wireless Client Utility

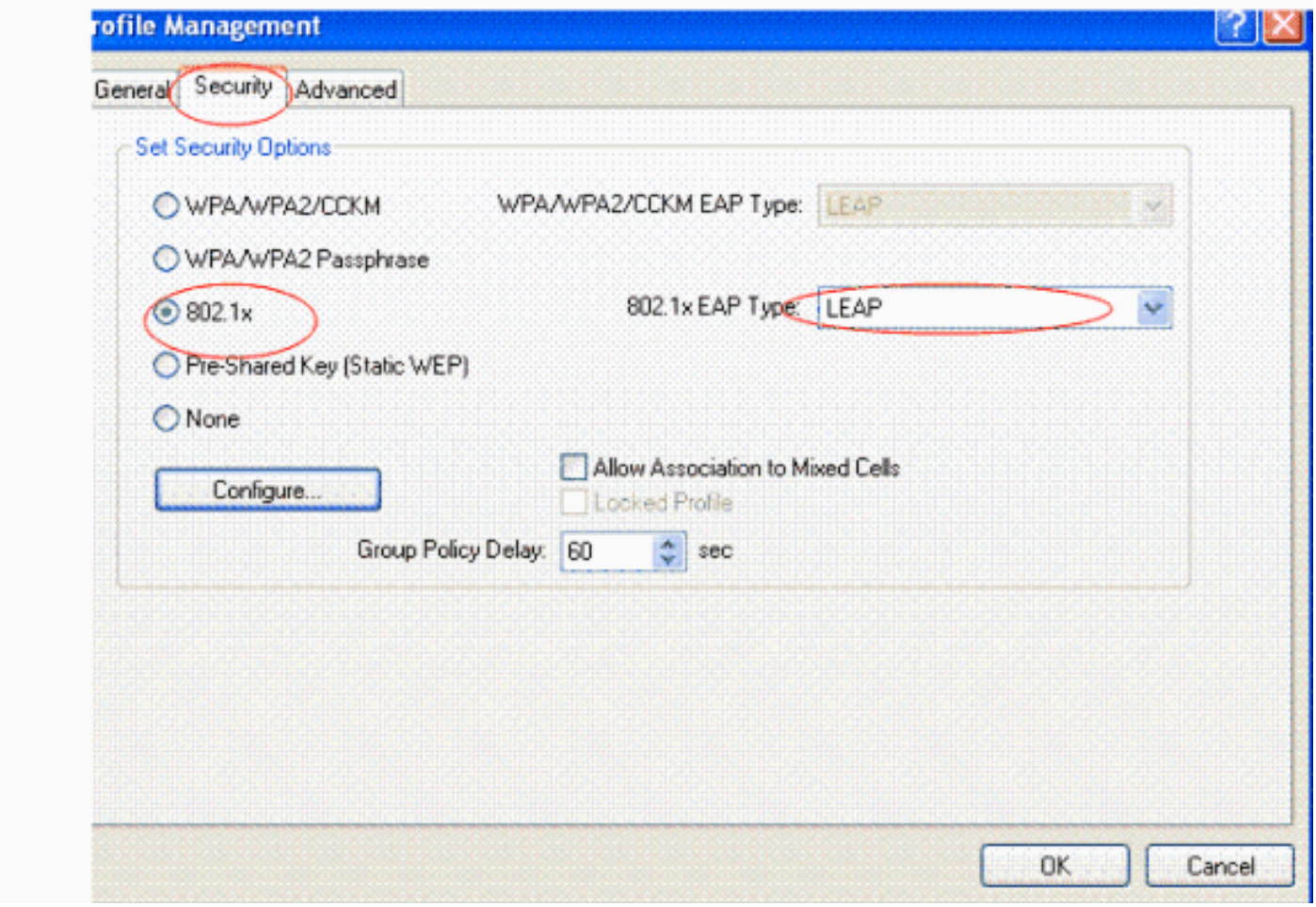
In questo documento viene usato ADU come utility client per la configurazione dei profili utente. Questa configurazione utilizza anche LEAP come protocollo di autenticazione. Configurare l'ADU come mostrato nell'esempio di questa sezione.

Per creare un nuovo profilo, dalla barra dei menu ADU scegliere **Gestione profili > Nuovo**.

Il client di esempio è configurato per far parte di SSID VLAN10. Questi diagrammi mostrano come configurare un profilo utente su un client:


Cisco Aironet Desktop Utility - Current Profile: Default
Action Options Help
Current Status
Profile Management
Diagnostics
Default
LAP
Ext.Web
New...
Modify...
Remove
Activate
Details
Network Type:
Security Mode:
Network Name 1 (SSID1):
Network Name 2 (SSID2):
Network Name 3 (SSID3):
Import...
Export...
Scan...
Auto Select Profiles
Order Profiles...


Profile Management
General
Security
Advanced
Profile Settings
Profile Name:
vlan10
Client Name:
WCS
Network Names
SSID1:
vlan10
SSID2:
SSID3:
OK
Cancel



Verifica

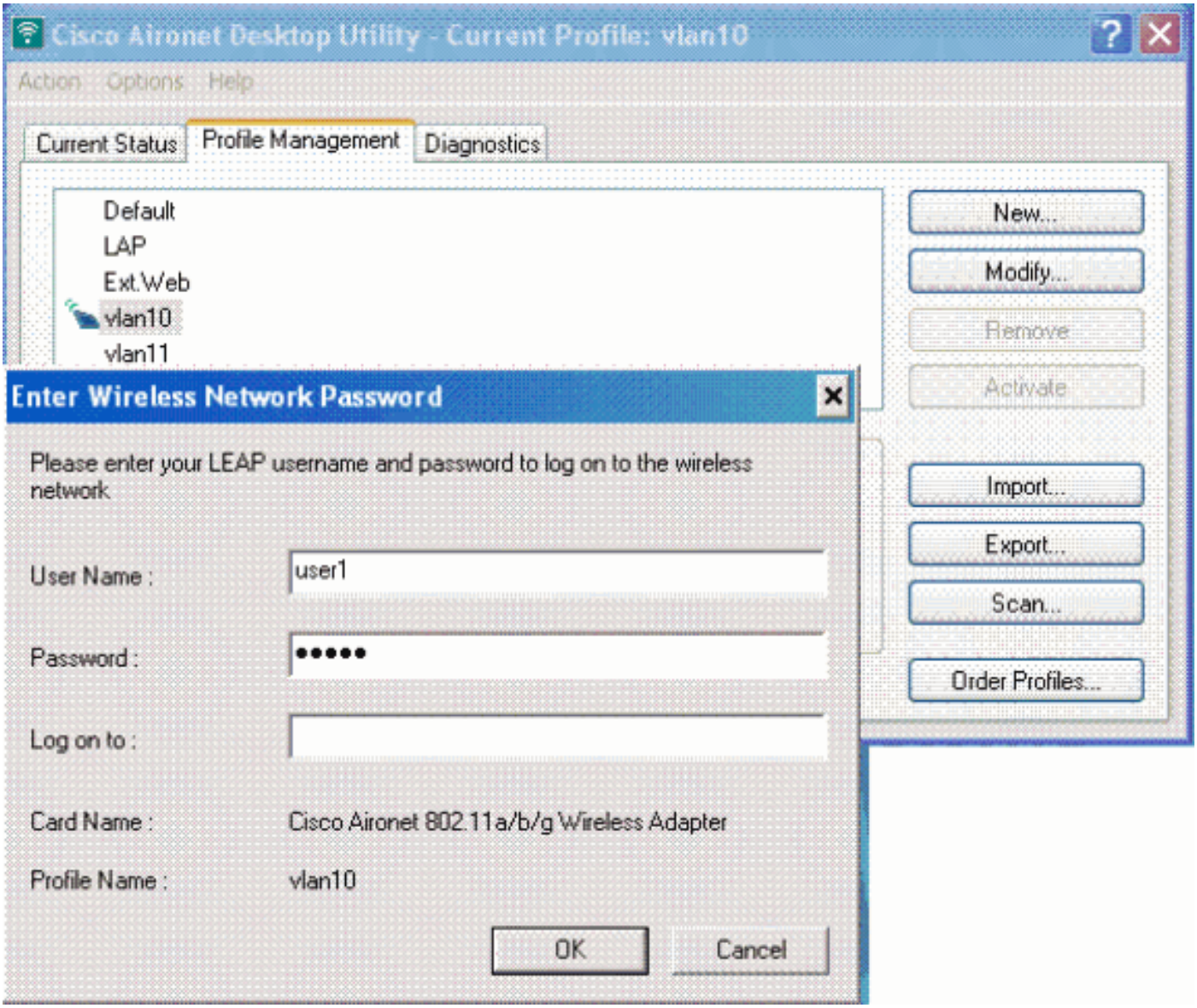
Attivare il profilo utente configurato nell'ADU. In base alla configurazione, viene richiesto di immettere un nome utente e una password. È inoltre possibile indicare all'ADU di utilizzare il nome utente e la password di Windows per l'autenticazione. Il client può ricevere l'autenticazione in diverse opzioni. È possibile configurare queste opzioni nella scheda Protezione > Configura del profilo utente creato.

Nell'esempio precedente, l'utente 1 è assegnato alla VLAN10 come specificato nel server RADIUS.

In questo esempio vengono utilizzati il nome utente e la password specificati dal client per ricevere l'autenticazione e per essere assegnati a una VLAN dal server RADIUS:

- Nome utente = utente1
- Password = utente1

Nell'esempio viene mostrato come richiedere il nome utente e la password alla VLAN10 SSID. Il nome utente e la password vengono immessi nell'esempio seguente:



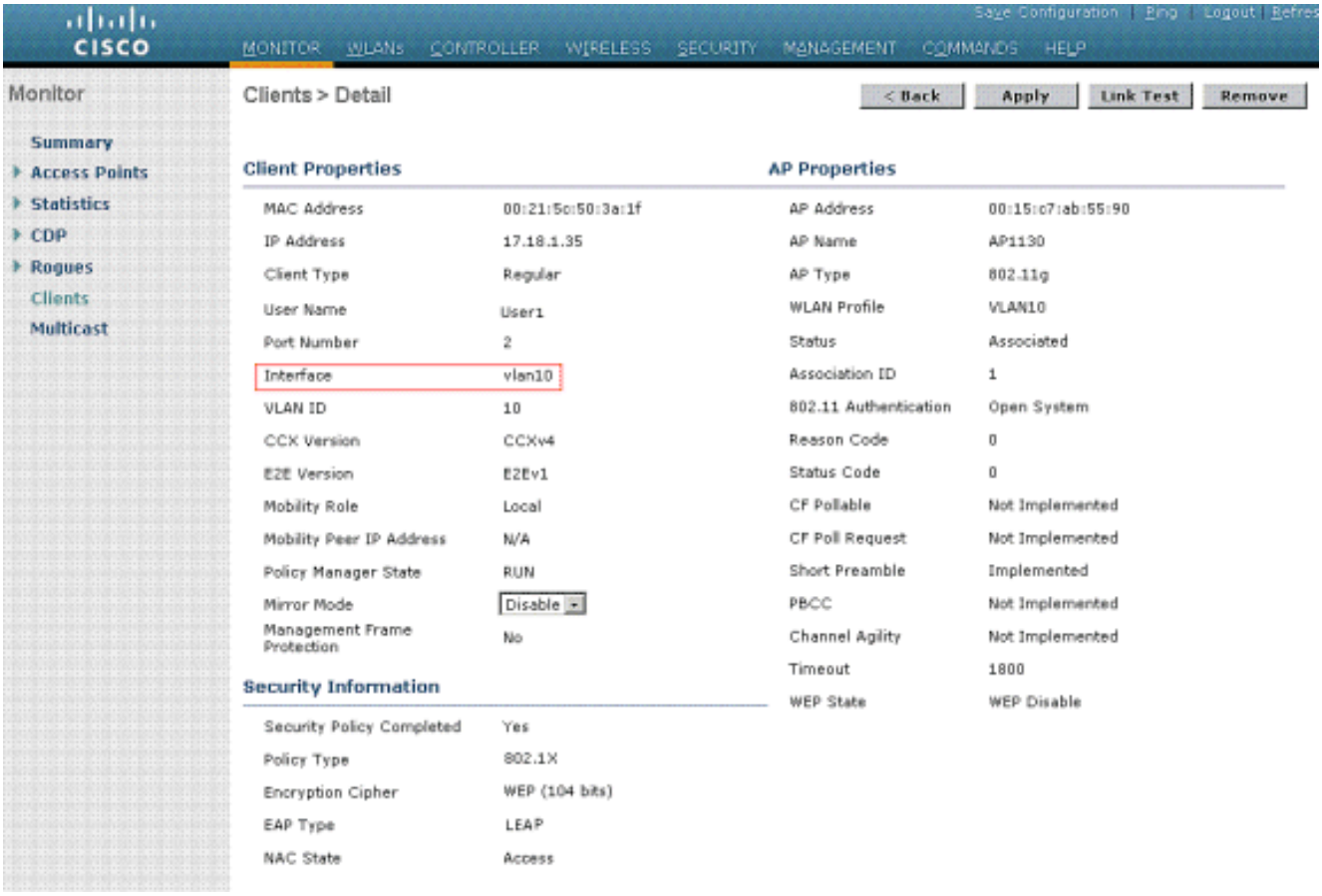
Se l'autenticazione e la convalida corrispondente hanno esito positivo, verrà visualizzato il messaggio di stato Operazione riuscita.

Quindi, è necessario verificare che il client sia assegnato alla VLAN corretta in base agli attributi RADIUS inviati. A tale scopo, effettuare i seguenti passaggi:

1. Dalla GUI del controller, selezionare **Wireless > AP**.
2. Fare clic su **Client**, visualizzato nell'angolo sinistro della finestra Access Point (AP).Vengono visualizzate le statistiche
client.

3. Fare clic su **Details** (Dettagli) per identificare i dettagli completi del client, come l'indirizzo IP, la VLAN a cui è assegnato e così via.In questo esempio vengono visualizzati i seguenti

dettagli del client
utente1:



Da questa finestra è possibile osservare che il client è assegnato alla VLAN10 in base agli attributi RADIUS configurati sul server RADIUS.**Nota:** se l'assegnazione della VLAN dinamica è basata sull'impostazione dell'**attributo VSA di Cisco Airespace**, il **nome** dell'**interfaccia la visualizzerà come admin**, come mostrato nell'esempio, nella pagina dei dettagli del client.

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

- **debug aaa events enable**: questo comando può essere usato per garantire il corretto trasferimento degli attributi RADIUS al client tramite il controller. Questa parte dell'output di debug garantisce la corretta trasmissione degli attributi RADIUS:

```
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[0]:
attribute 64, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[1]:
attribute 65, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[2]:
attribute 81, vendorId 0, valueLen 3
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[3]:
attribute 79, vendorId 0, valueLen 32
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Received EAP Attribute
(code=2, length=32,id=0) for mobile 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00000000: 02 00 00 20 11 01 00 18
4a 27 65 69 6d e4 05 f5
........J'eim...00000010: d0 98 0c cb 1a 0c 8a 3c
........44 a9 da 6c 36 94 0a f3  <D..l6...
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[4]:
attribute 1, vendorId 9, valueLen 16
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[5]:
attribute 25, vendorId 0, valueLen 28
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[6]:
attribute 80, vendorId 0, valueLen 16
```

```
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Type 16777229
should be 13 for STA 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Medium-Type 16777222
should be 6 for STA 00:40:96:ac:e6:57
Fri Jan 20 02:30:00 2006: 00:40:96:ac:e6:57 Station 00:40:96:ac:e6:57
setting dot1x reauth timeout = 1800
```

- Questi comandi possono essere utili anche:**debug dot1x aaa enableabilitazione pacchetti debug aaa**

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Nota: l'assegnazione della VLAN dinamica non funziona per l'autenticazione Web da un WLC.

Informazioni correlate

- Autenticazione EAP con server RADIUS
- Cisco LEAP
- Guida alla configurazione di Cisco Wireless LAN Controller, versione 4.0
- Documentazione e supporto tecnico – Cisco Systems