Configurazione di un WLC e di un ACS per l'autenticazione degli utenti di gestione

Sommario

Introduzione

In questo documento viene descritto come configurare un WLC e un Cisco Secure ACS in modo che il server AAA possa autenticare gli utenti di gestione sul controller.

Prerequisiti

Requisiti

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

- Informazioni su come configurare i parametri di base sui WLC
- Informazioni su come configurare un server RADIUS come Cisco Secure ACS

Componenti usati

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

- Cisco Wireless LAN Controller 4400 con versione 7.0.216.0
- Cisco Secure ACS con software versione 4.1 e utilizzato come server RADIUS in questa configurazione.

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

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

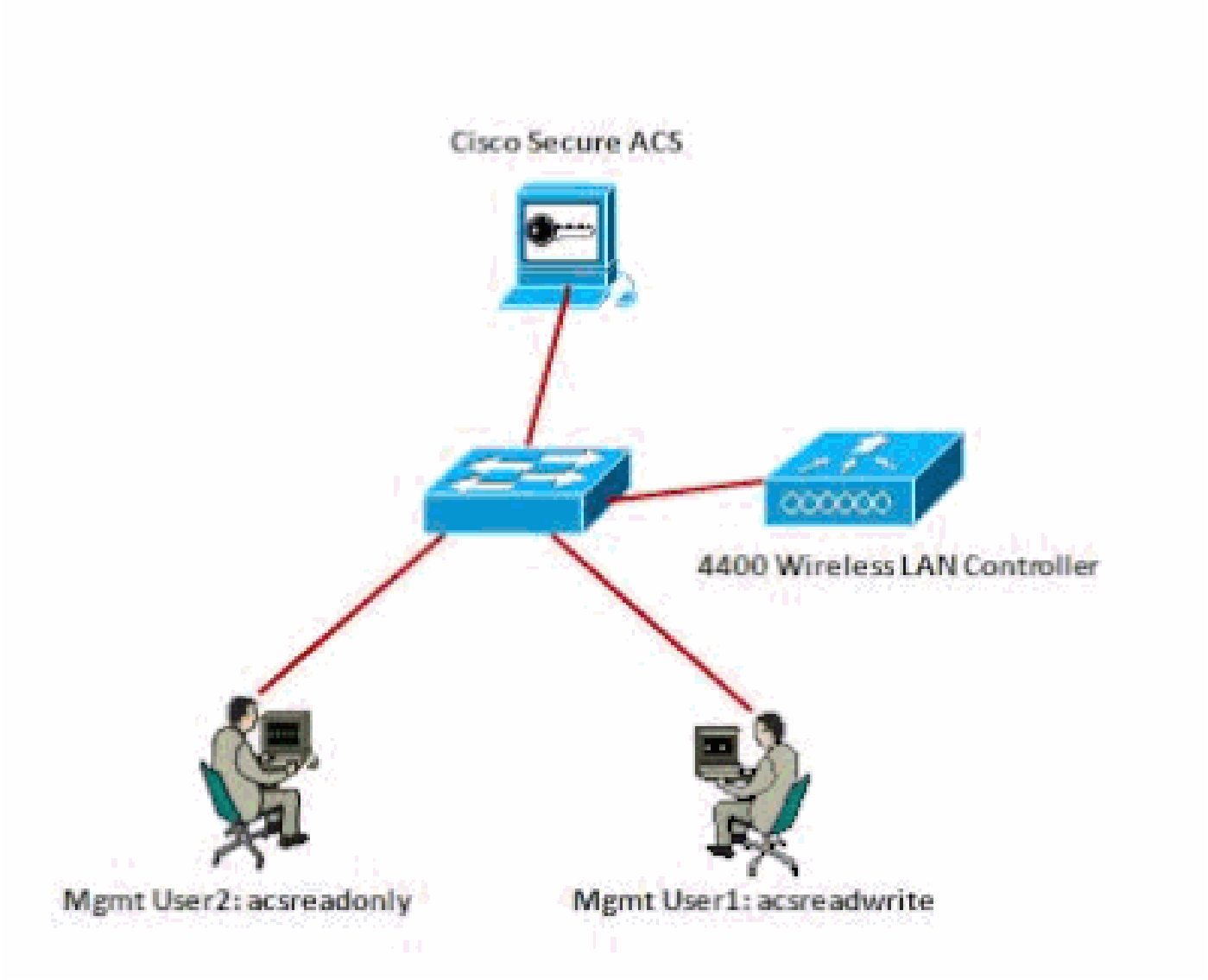
In questo documento viene spiegato come configurare un controller WLC (Wireless LAN Controller) e un server di controllo dell'accesso (Cisco Secure ACS) in modo che il server AAA (Authentication, Authorization, and Accounting) possa autenticare gli utenti di gestione sul controller. Nel documento viene spiegato anche come diversi utenti di gestione possono ricevere privilegi diversi con gli attributi specifici del fornitore (VSA) restituiti dal server RADIUS Cisco Secure ACS.

Configurazione

In questa sezione vengono presentate le informazioni su come configurare il WLC e l'ACS per lo scopo descritto in questo documento.

Esempio di rete

Il documento usa la seguente configurazione di rete:



Esempio di rete

In questo esempio di configurazione vengono utilizzati i seguenti parametri:

- Indirizzo IP di Cisco Secure ACS —172.16.1.1/255.255.0.0
- Indirizzo IP dell'interfaccia di gestione del controller: 172.16.1.30/255.255.0.0
- Chiave segreta condivisa utilizzata sul punto di accesso (AP) e sul server RADIUS: asdf1234
- Queste sono le credenziali dei due utenti configurati da questo esempio su ACS:
    - Nome utente - acsreadwrite

      Password - acsreadwrite
    - Nome utente - acsreadonly

      Password - acsreadonly

È necessario configurare il WLC e Cisco Secure Cisco ACS per:

- A qualsiasi utente che accede al WLC con il nome utente e la password acsreadwrite viene concesso l'accesso amministrativo completo al WLC.
- A tutti gli utenti che accedono al WLC con il nome utente e la password acsreadonly viene concesso l'accesso in sola lettura al WLC.

Configurazioni

In questo documento vengono usate le seguenti configurazioni:

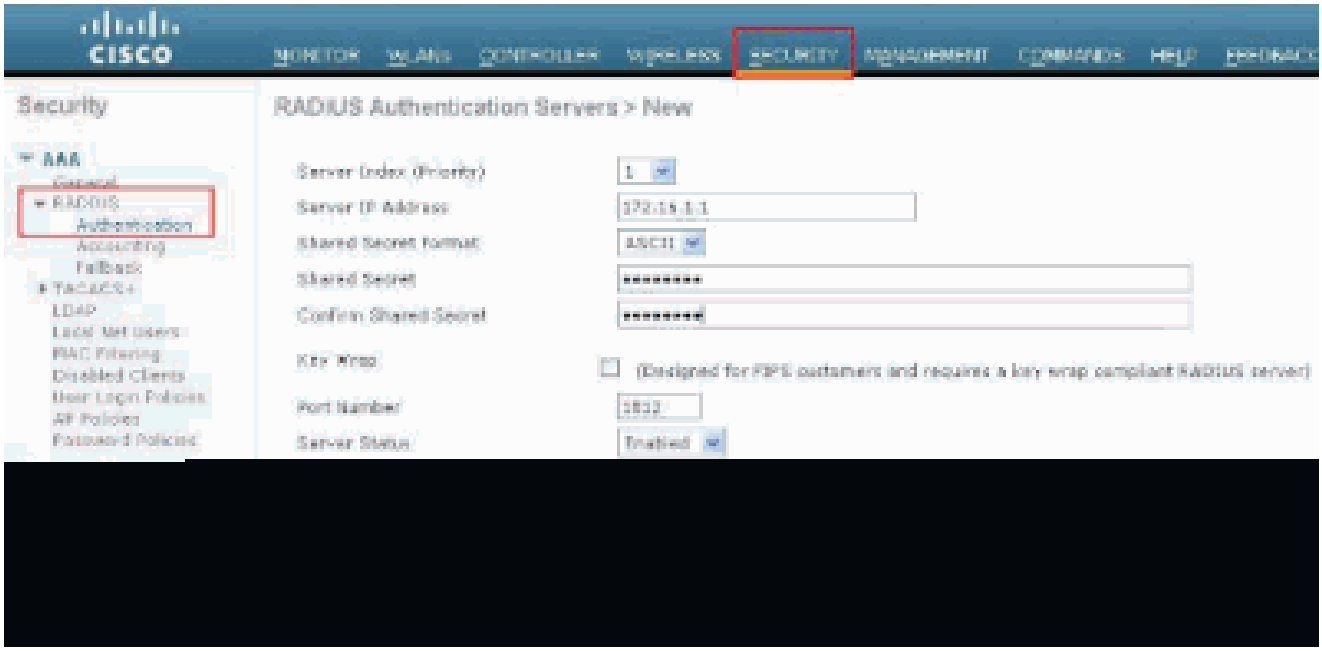
- Configurazione WLC
- Configurazione Cisco Secure ACS

Configurazione WLC

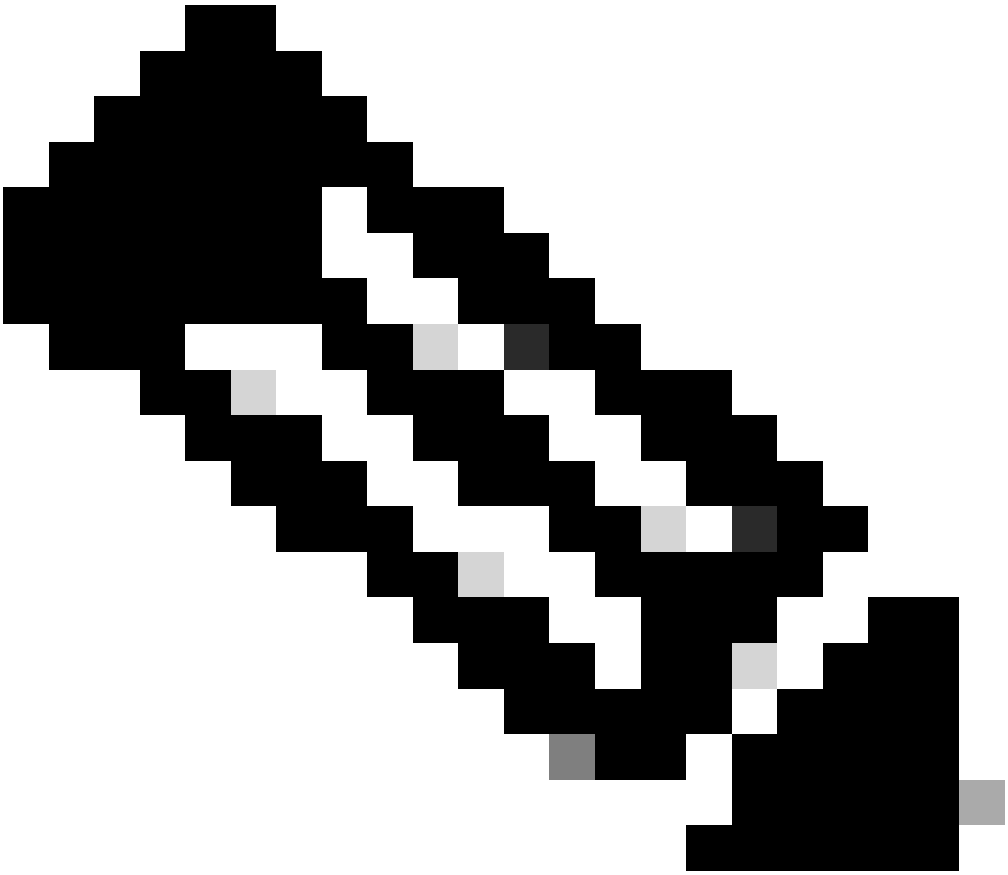
Configurare il WLC per accettare la gestione tramite il server Cisco Secure ACS

Per configurare il WLC in modo che comunichi con il server RADIUS, completare la procedura seguente:

1. Dall'interfaccia utente del WLC, fare clic su Security (Sicurezza). Dal menu a sinistra, fare clic su RADIUS > Authentication (Autenticazione). Viene visualizzata la pagina Server di autenticazione RADIUS. Per aggiungere un nuovo server RADIUS, fare clic su Nuovo. Nella pagina Server di autenticazione RADIUS > Nuovo , immettere i parametri specifici del server RADIUS. Ecco un esempio.

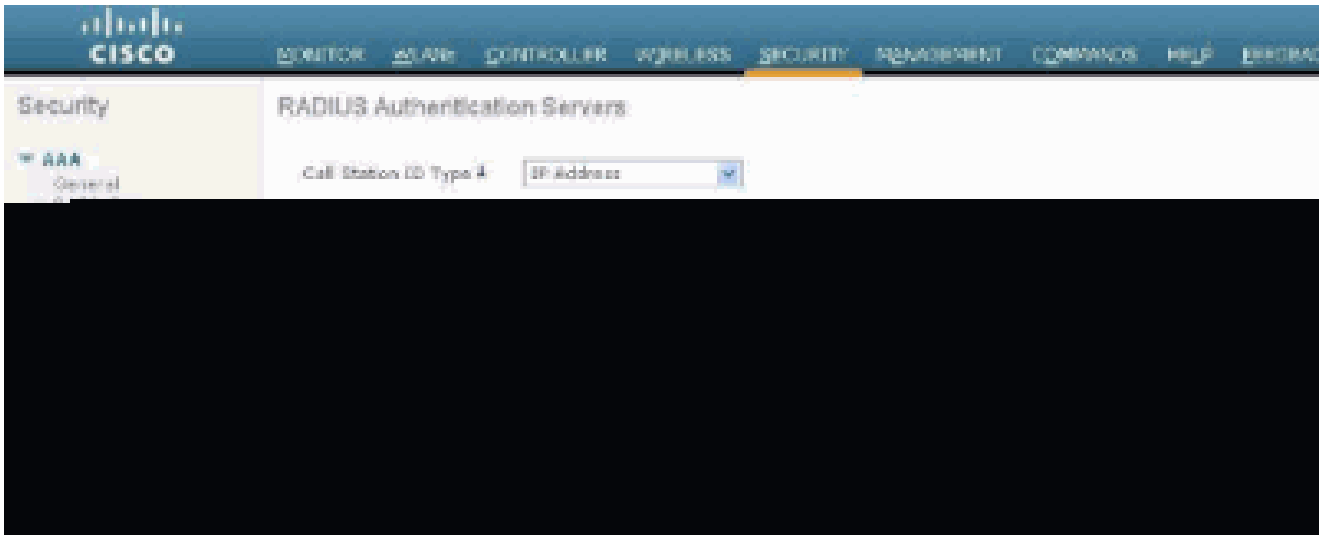


2. Selezionare il pulsante di opzione Management per consentire al server RADIUS di autenticare gli utenti che accedono al WLC.



Nota: verificare che il segreto condiviso configurato in questa pagina corrisponda al segreto condiviso configurato nel server RADIUS. Solo in questo caso il WLC può comunicare con il server RADIUS.

3. Verificare se il WLC è configurato per essere gestito da Cisco Secure ACS. A tale scopo, fare clic su Security (Sicurezza) dall'interfaccia utente del WLC. La finestra GUI risultante appare simile a questo esempio.



È possibile notare che la casella di controllo Gestione è abilitata per il server RADIUS 172.16.1.1. Ciò dimostra che ACS è autorizzato ad autenticare gli utenti di gestione sul WLC.

Configurazione Cisco Secure ACS

Per configurare il server ACS, completare la procedura descritta nelle sezioni seguenti:

1. Aggiungere il WLC come client AAA al server RADIUS.
2. Configurare gli utenti e gli attributi IETF RADIUS appropriati.
3. Configurare un utente con accesso in lettura/scrittura.
4. Configurare un utente con accesso in sola lettura.

Aggiungere il WLC come client AAA al server RADIUS

Completare questi passaggi per aggiungere il WLC come client AAA nel Cisco Secure ACS:

1. Dall'interfaccia utente di ACS, fare clic su Network Configuration (Configurazione di rete).
2. In Client AAA, fare clic su Add Entry (Aggiungi voce).
3. Nella finestra Add AAA Client, immettere il nome host del WLC, l'indirizzo IP del WLC e una chiave segreta condivisa.

   Nell'esempio, le impostazioni sono le seguenti:

   - Nome host client AAA: WLC-4400
   - 172.16.1.30/16 è l'indirizzo IP del client AAA, in questo caso il WLC.
   - La chiave segreta condivisa è "asdf1234".

Finestra Aggiungi client AAA

Questa chiave segreta condivisa deve essere uguale alla chiave segreta condivisa configurata sul WLC.

4. Dal menu a discesa Autentica con, scegliere RADIUS (Cisco Airespace).
5. Per salvare la configurazione, fare clic su Submit + Restart (Invia e riavvia).

Configurazione degli utenti e degli attributi IETF RADIUS appropriati

Per autenticare un utente tramite un server RADIUS, per l'accesso e la gestione dei controller, è necessario aggiungere l'utente al database RADIUS con l'attributoService-Typeset RADIUS IETF al valore appropriato in base ai privilegi dell'utente.

- Per impostare i privilegi di lettura/scrittura per l'utente, impostare Service-TypeAttribute su Administrative.
- Per impostare i privilegi di sola lettura per l'utente, impostare Service-TypeAttribute su NAS-Prompt.

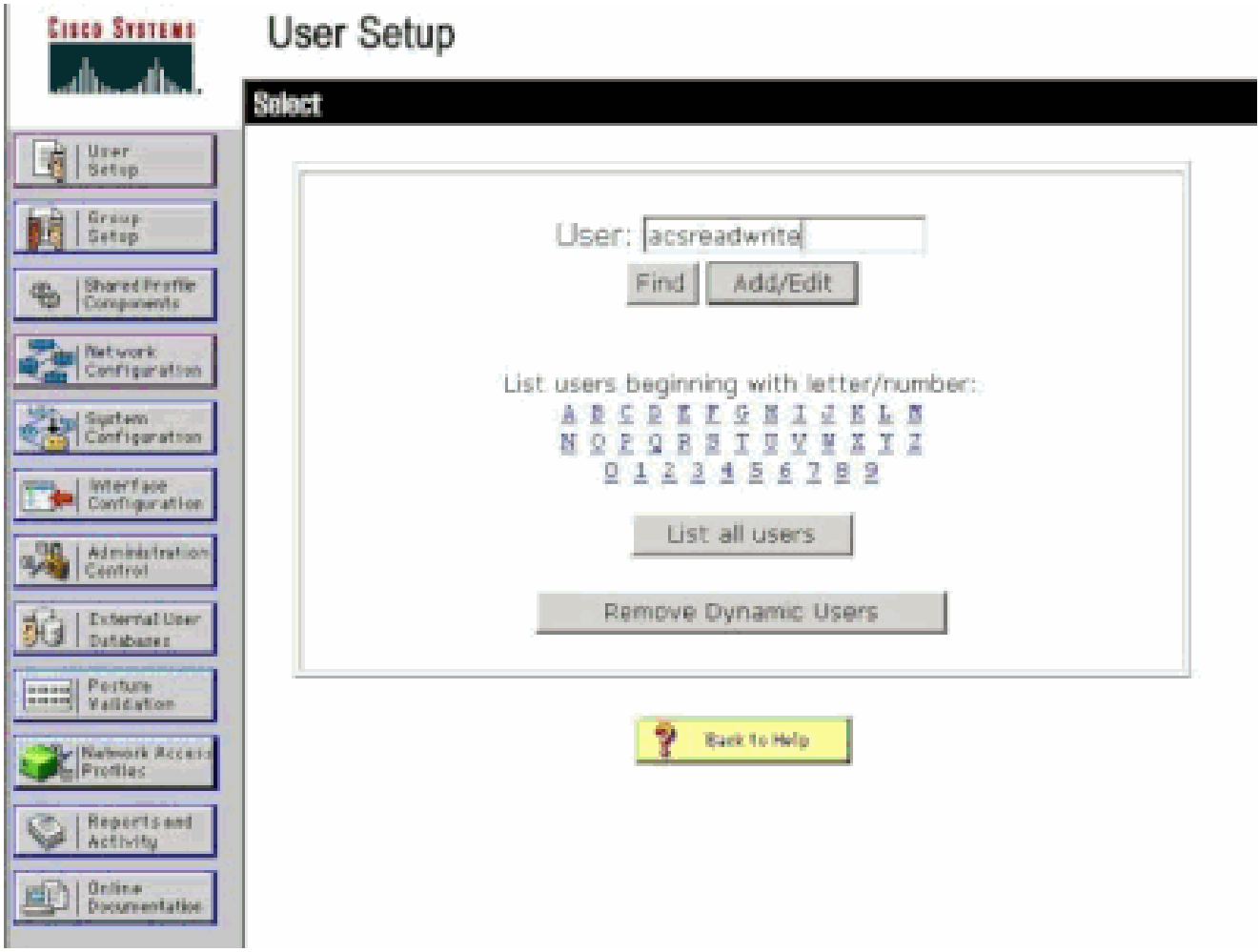
Configurare un utente con accesso in lettura/scrittura

Nel primo esempio viene mostrata la configurazione di un utente con accesso completo al WLC. Quando l'utente tenta di accedere al controller, il server RADIUS esegue l'autenticazione e fornisce all'utente accesso amministrativo completo.

Nell'esempio, il nome utente e la password sono acsreadwrite.

Completare questi passaggi su Cisco Secure ACS.

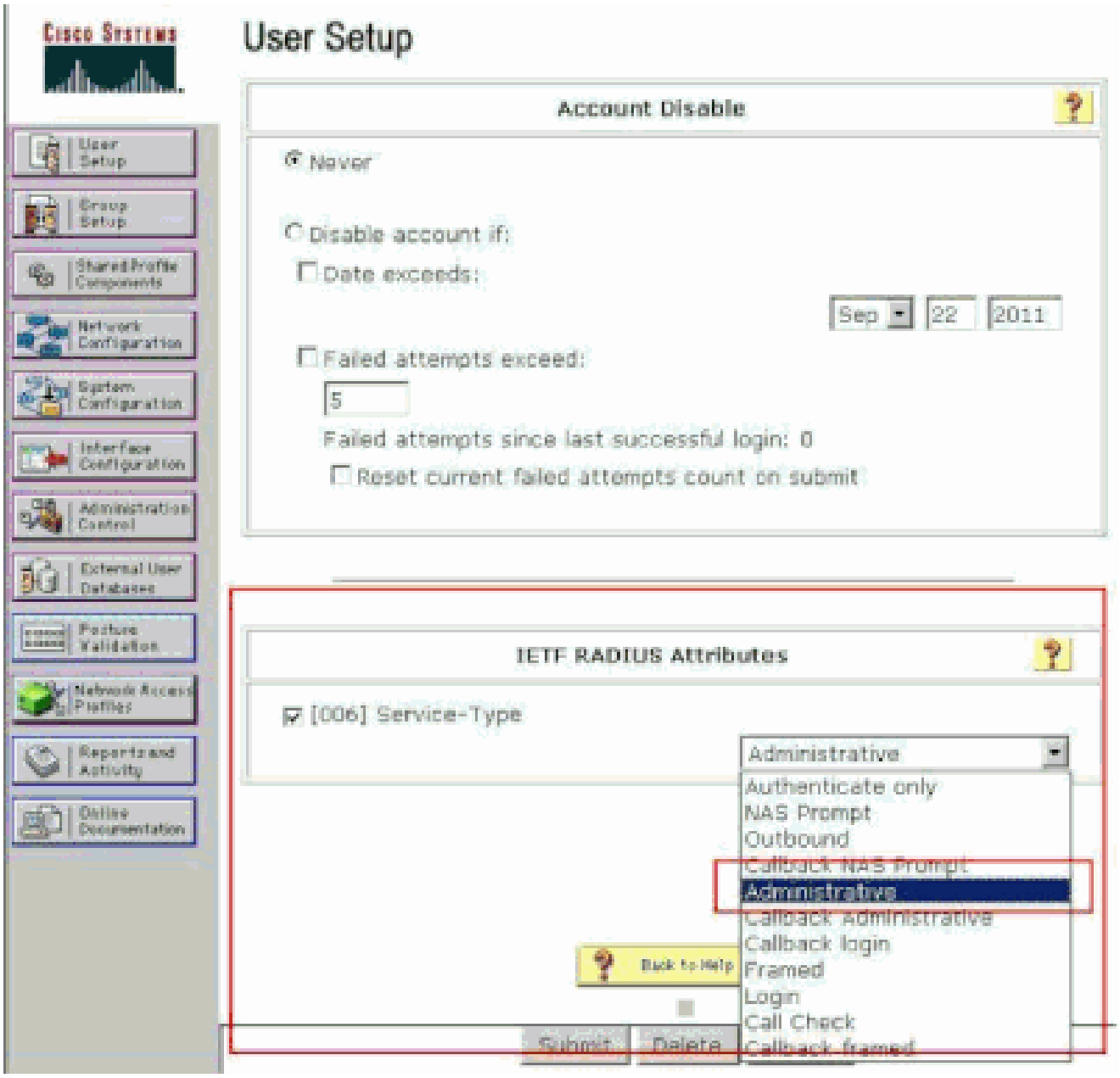
1. Dalla GUI di ACS, fare clic su User Setup (Configurazione utente).
2. Digitare il nome utente da aggiungere ad ACS come mostrato nella finestra di esempio.



Finestra Impostazione utente

3. Fare clic su Add/Edit (Aggiungi/Modifica) per accedere alla pagina User Edit (Modifica utente).
4. Nella pagina Modifica utente specificare il nome reale, la descrizione e la password dell'utente.
5. Scorrere verso il basso fino all'impostazione Attributi RADIUS IETF e selezionare Attributo Service-Type.
6. Poiché in questo esempio è necessario concedere all'utente acsreadwrite l'accesso completo, scegliere Amministrativo dal menu a discesa Service-Type e fare clic su Submit.

   In questo modo si assicura che questo particolare utente disponga dell'accesso in lettura/scrittura al WLC.



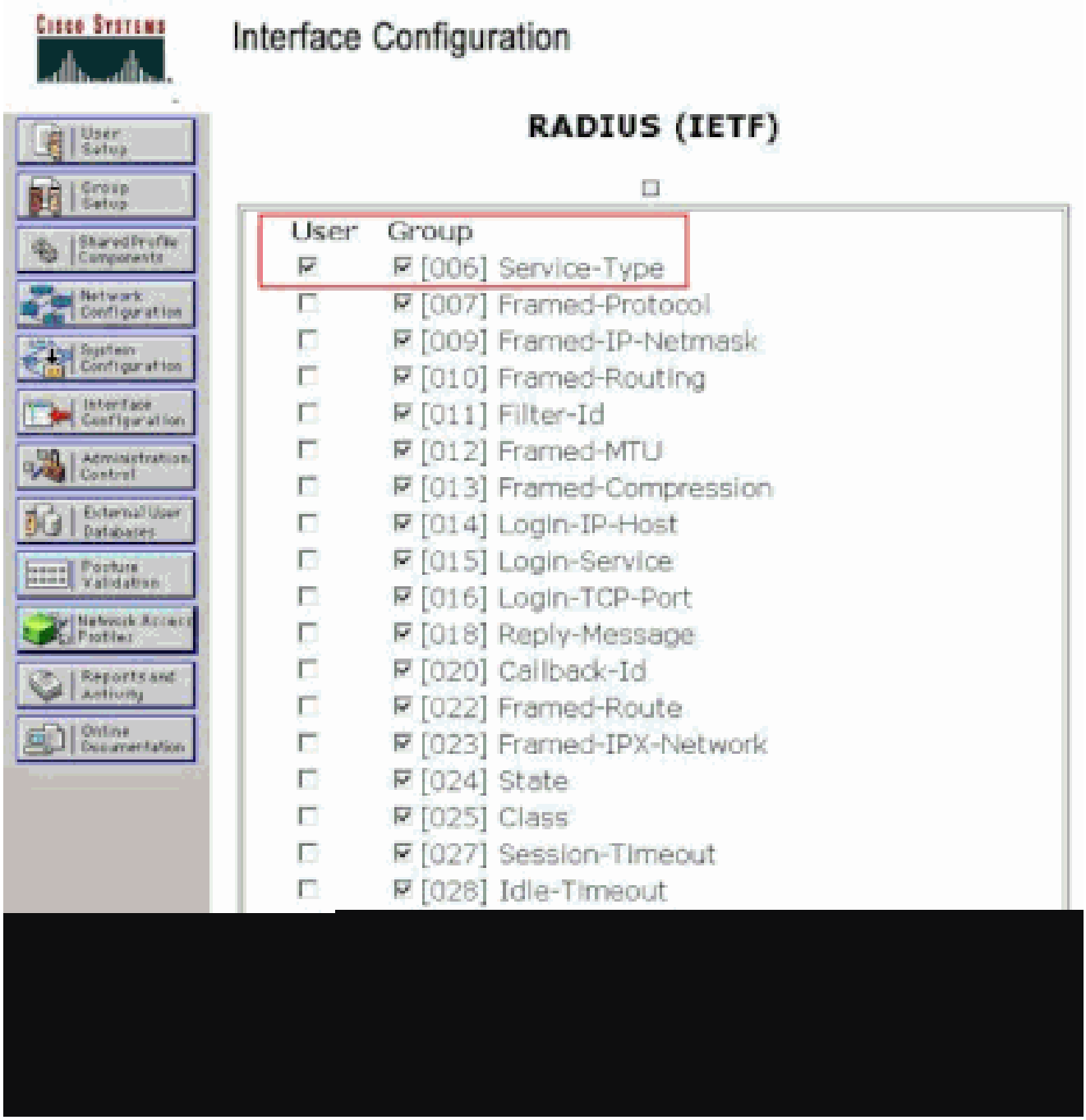
Impostazioni attributi RADIUS ETF

A volte questo attributo Service-Type non è visibile nelle impostazioni utente. In questi casi, completare questi passaggi per renderli visibili.

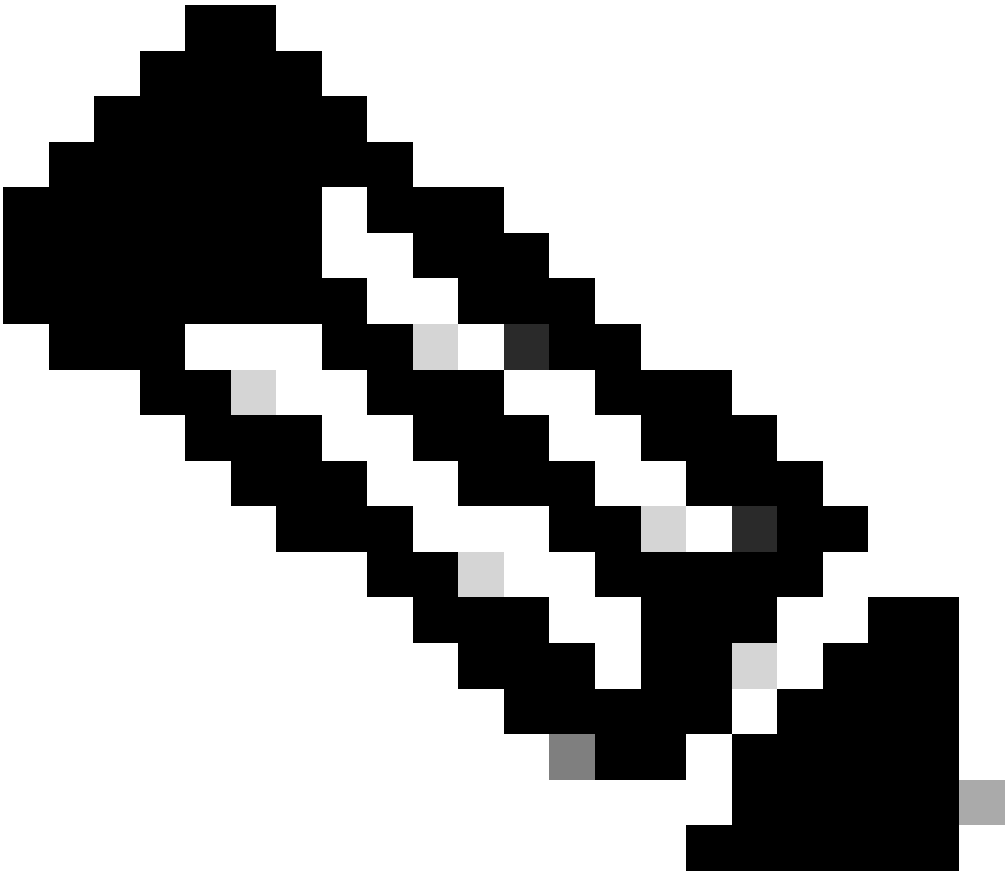
1. Dalla GUI di ACS, selezionare Interface Configuration > RADIUS (IETF) per abilitare gli attributi IETF nella finestra User Configuration.

   Viene visualizzata la pagina Impostazioni RADIUS (IETF).

2. Nella pagina Impostazioni RADIUS (IETF) è possibile attivare l'attributo IETF che deve essere visibile in Impostazioni utente o gruppo. Per questa configurazione, selezionare Service-Type per la colonna User e fare clic su Submit. In questa finestra viene illustrato un esempio.



Pagina Impostazioni RADIUS (IETF)



Nota: in questo esempio viene specificata l'autenticazione per singolo utente. È inoltre possibile eseguire l'autenticazione in base al gruppo a cui appartiene un determinato utente. In questi casi, attivare la casella di controllo Raggruppa in modo che l'attributo sia visibile in Impostazioni gruppo. Inoltre, se l'autenticazione avviene su base di gruppo, è necessario assegnare gli utenti a un determinato gruppo e configurare gli attributi IETF dell'impostazione di gruppo in modo da fornire i privilegi di accesso agli utenti di tale gruppo. Per informazioni dettagliate su come configurare e gestire i gruppi, fare riferimento a Gestione gruppi.

Configurare un utente con accesso in sola lettura

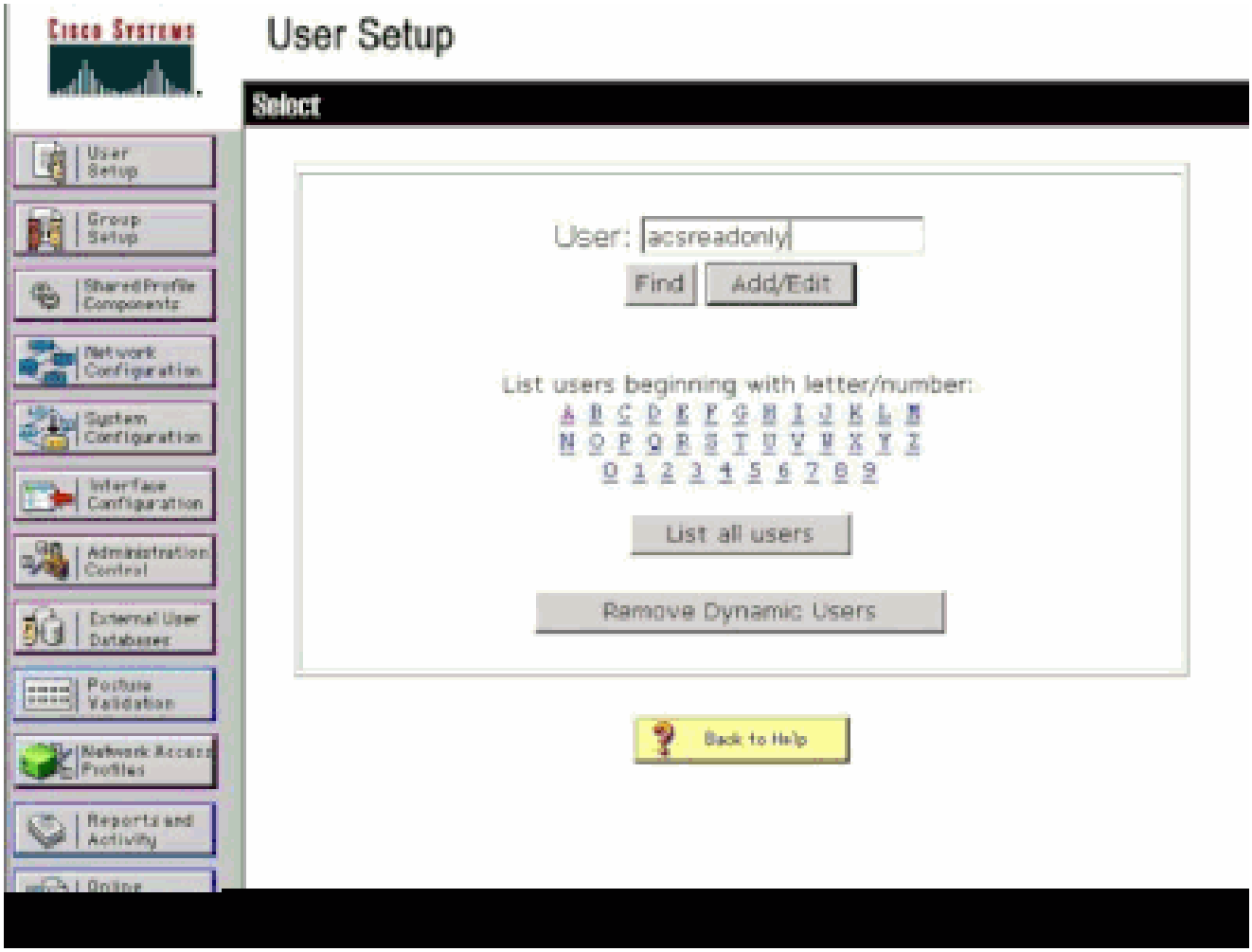
Nell'esempio viene mostrata la configurazione di un utente con accesso in sola lettura al WLC. Quando l'utente tenta di accedere al controller, il server RADIUS esegue l'autenticazione e fornisce all'utente accesso in sola lettura.

Nell'esempio, il nome utente e la password sono acsreadonly.

Completare questi passaggi su Cisco Secure ACS:

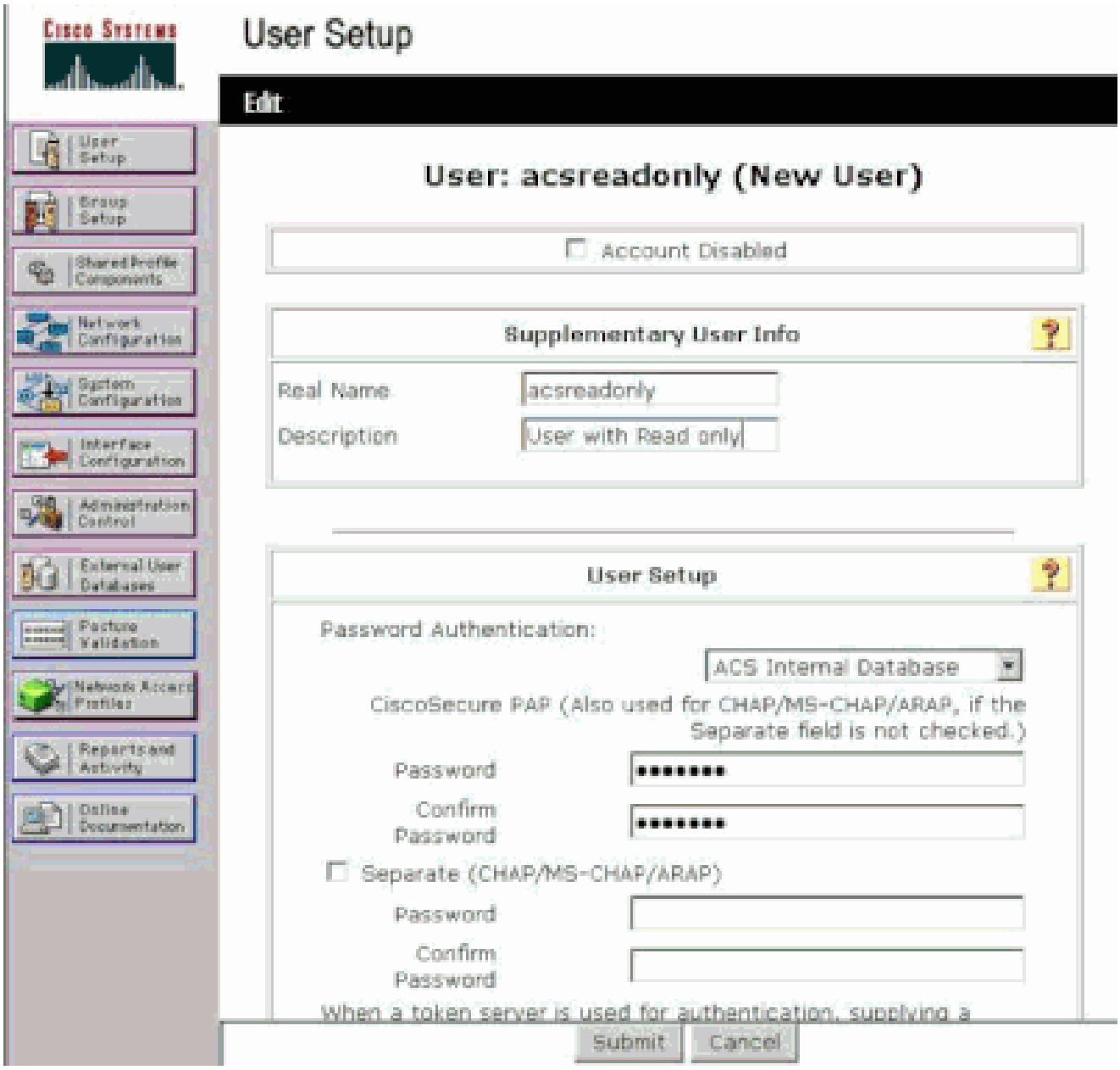
1. Dalla GUI di ACS, fare clic su User Setup (Configurazione utente).

2. Digitare il nome utente che si desidera aggiungere al server ACS e fare clic su Add/Edit (Aggiungi/Modifica) per accedere alla pagina User Edit (Modifica utente).



Aggiungi un nome utente

3. Specificare il nome reale, la descrizione e la password dell'utente. In questa finestra viene illustrato un esempio.

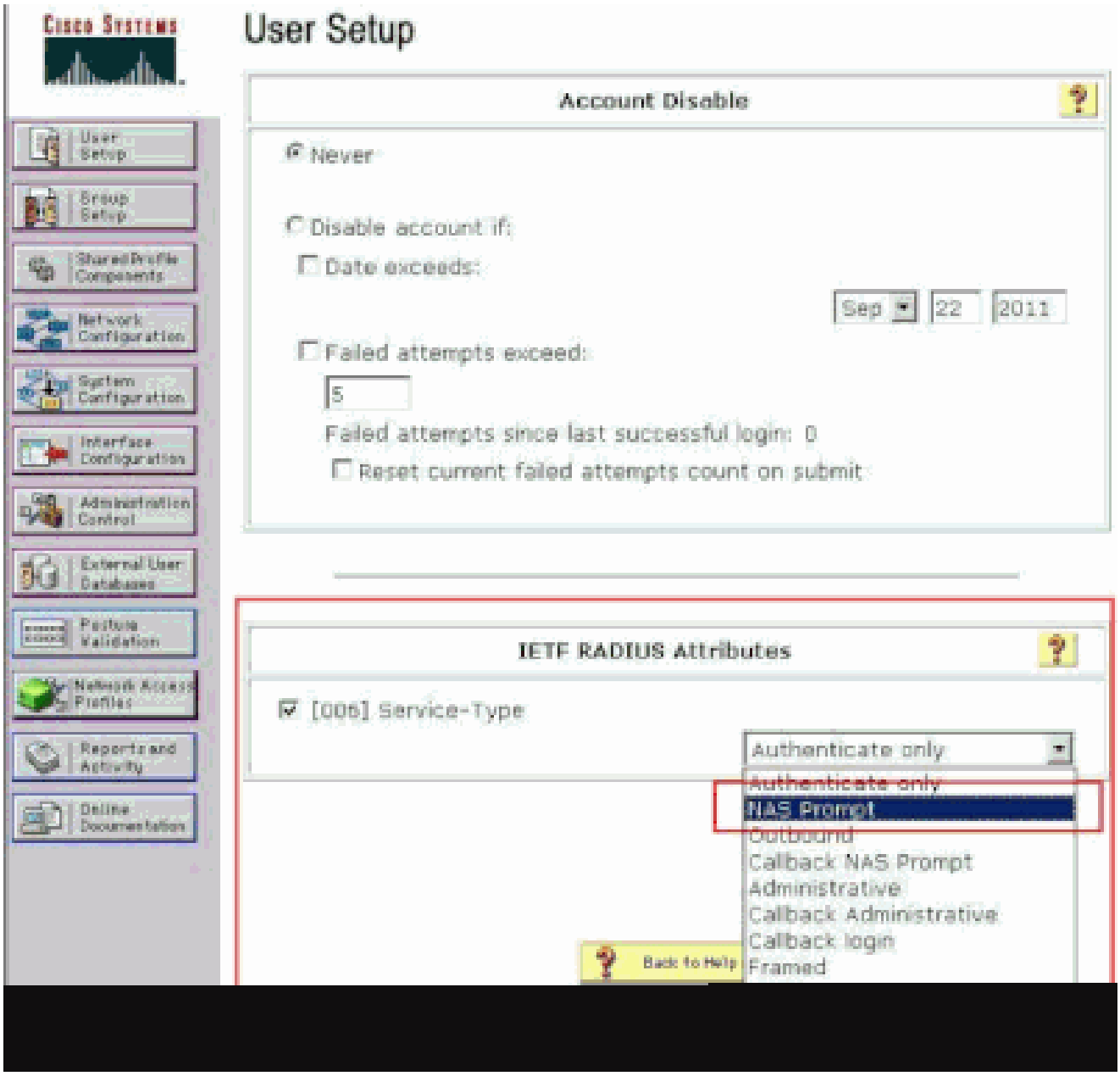


Fornire il vero nome, la descrizione e la password dell'utente aggiunto

4. Scorrere verso il basso fino all'impostazione Attributi RADIUS IETF e selezionare Attributo Service-Type.

5. Poiché, in questo esempio, l'utente acsreadonly deve disporre dell'accesso in sola lettura, scegliere NAS Prompt dal menu a discesa Service-Type e fare clic su Submit (Invia).

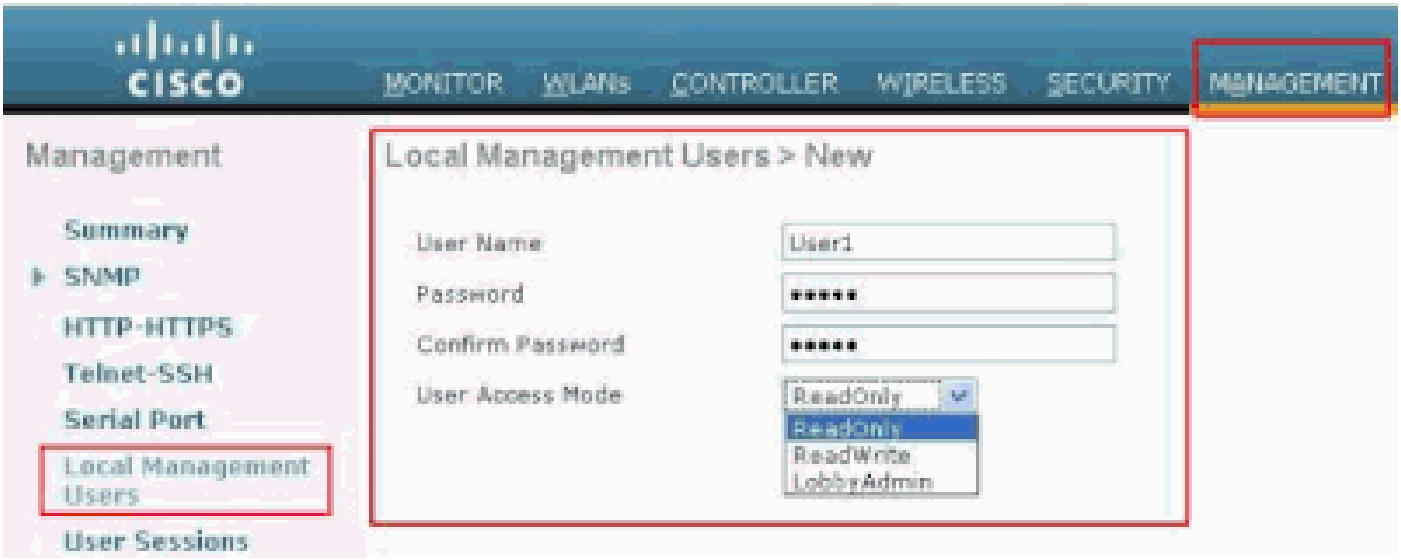
   In questo modo si garantisce che questo particolare utente abbia accesso in sola lettura al WLC.



Verifica attributo Service-Type

Gestire il WLC localmente e tramite il server RADIUS

È possibile anche configurare gli utenti di gestione localmente sul WLC. Questa operazione può essere eseguita dalla GUI del controller, in Gestione > Utenti gestione locale.



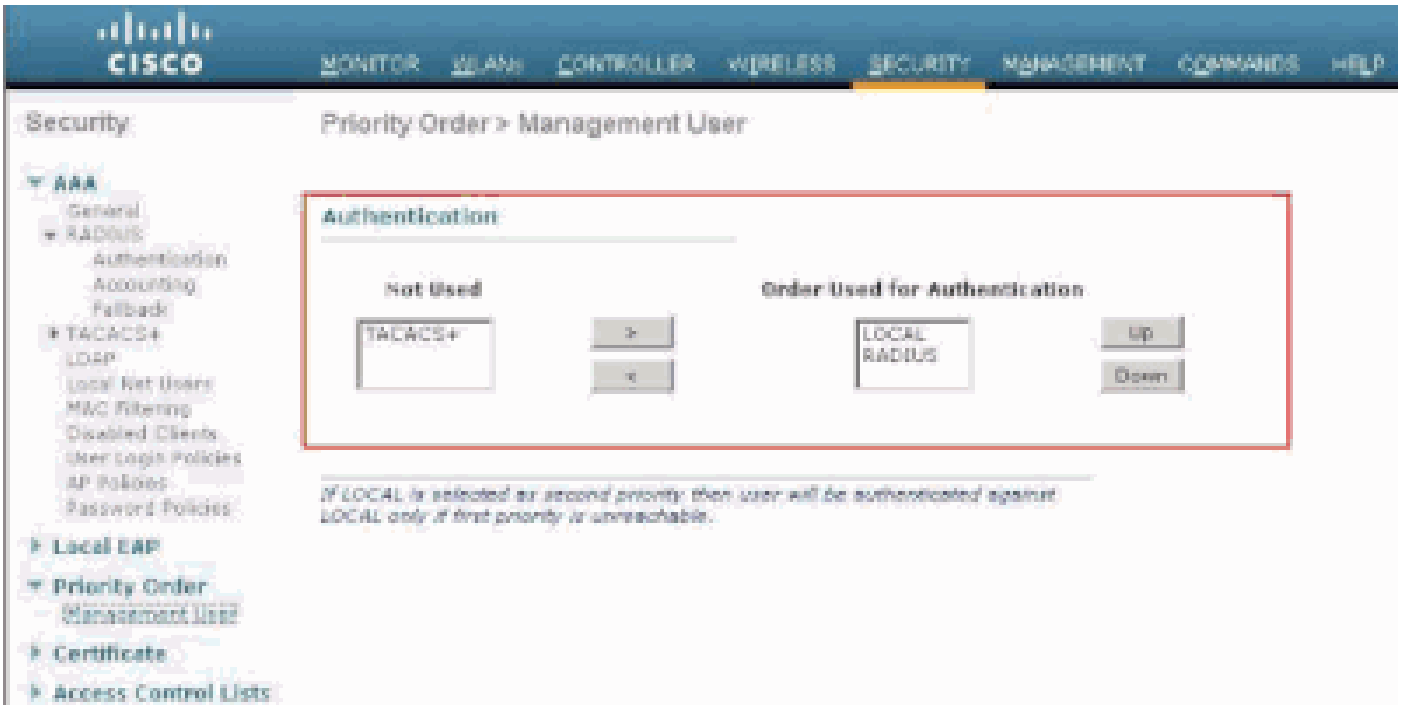
Configurare gli utenti di gestione localmente sul WLC

Si supponga che il WLC sia configurato con gli utenti di gestione sia localmente che nel server RADIUS con la casella di controllo Gestione abilitata. In uno scenario di questo tipo, per impostazione predefinita, quando un utente tenta di accedere al WLC, il WLC si comporta nel modo seguente:

1. Il WLC esamina innanzitutto gli utenti di gestione locali definiti per convalidare l'utente. Se l'utente è presente nell'elenco locale, consente l'autenticazione per l'utente. Se l'utente non viene visualizzato localmente, cerca nel server RADIUS.

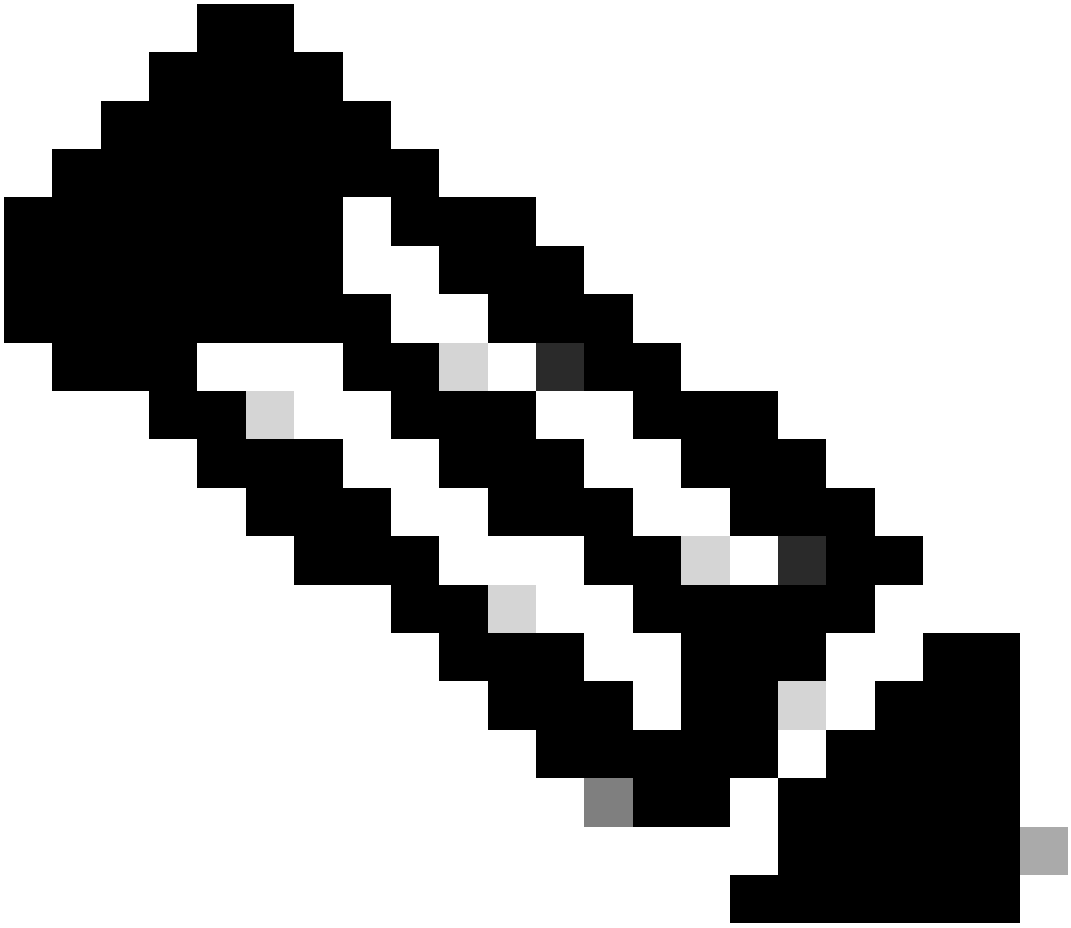
2. Se lo stesso utente esiste sia localmente che nel server RADIUS ma con privilegi di accesso diversi, il WLC autentica l'utente con i privilegi specificati localmente. In altre parole, la configurazione locale sul WLC ha sempre la precedenza rispetto al server RADIUS.

L'ordine di autenticazione per gli utenti di gestione può essere modificato sul WLC. A tale scopo, dalla pagina Sicurezza del WLC, fare clic su Ordine di priorità > Utente di gestione. Da questa pagina è possibile specificare l'ordine di autenticazione. Ecco un esempio.



Selezione utente gestione" />

Ordine di priorità > Selezione utente gestione



Nota: se si seleziona LOCAL come seconda priorità, l'utente viene autenticato con questo metodo solo se il metodo definito come prima priorità (RADIUS/ TACACS) non è raggiungibile.

Verifica

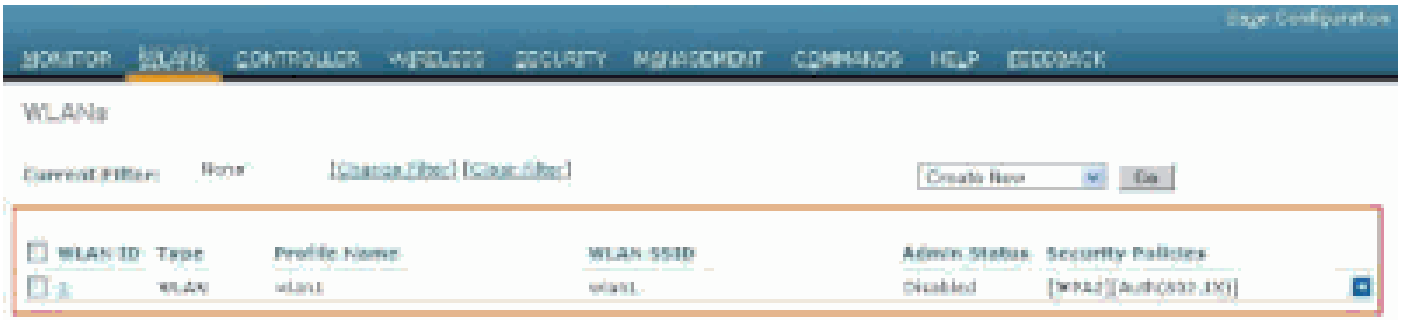
Per verificare il corretto funzionamento della configurazione, accedere al WLC dalla CLI o in modalità GUI (HTTP/HTTPS). Quando viene visualizzato il prompt di accesso, digitare il nome utente e la password come configurati in Cisco Secure ACS.

Se le configurazioni sono corrette, l'autenticazione nel WLC è riuscita.

È inoltre possibile verificare se all'utente autenticato vengono applicate le restrizioni di accesso specificate da ACS. A tal fine, accedere alla GUI del WLC tramite HTTP/HTTPS (verificare che il WLC sia configurato per consentire HTTP/HTTPS).

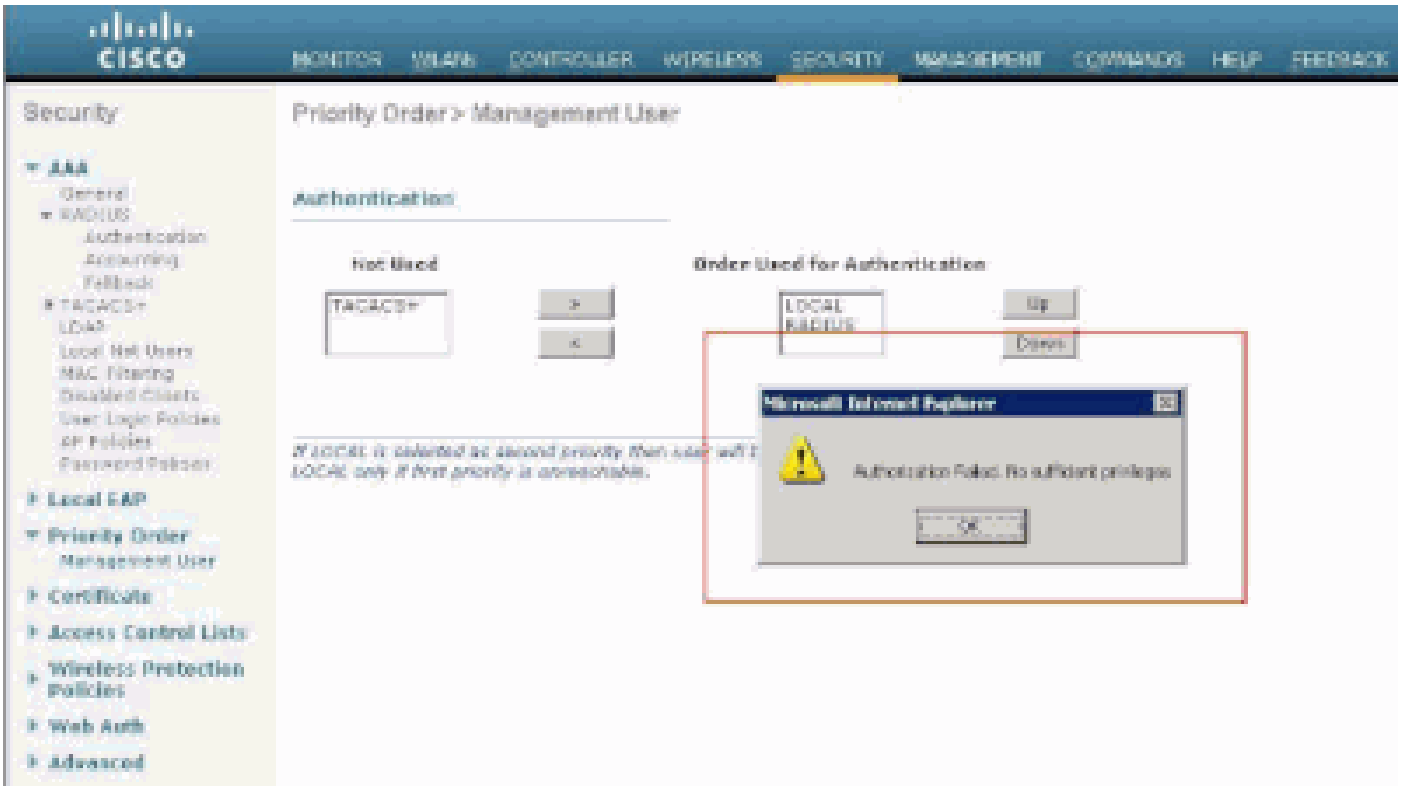
Un utente con accesso in lettura/scrittura impostato in ACS ha diversi privilegi configurabili nel

WLC. Ad esempio, un utente di lettura/scrittura ha il privilegio di creare una nuova WLAN nella pagina WLAN del WLC. In questa finestra viene illustrato un esempio.



Privilegi configurabili nel WLC

Quando un utente con privilegi di sola lettura tenta di modificare la configurazione sul controller, viene visualizzato questo messaggio.



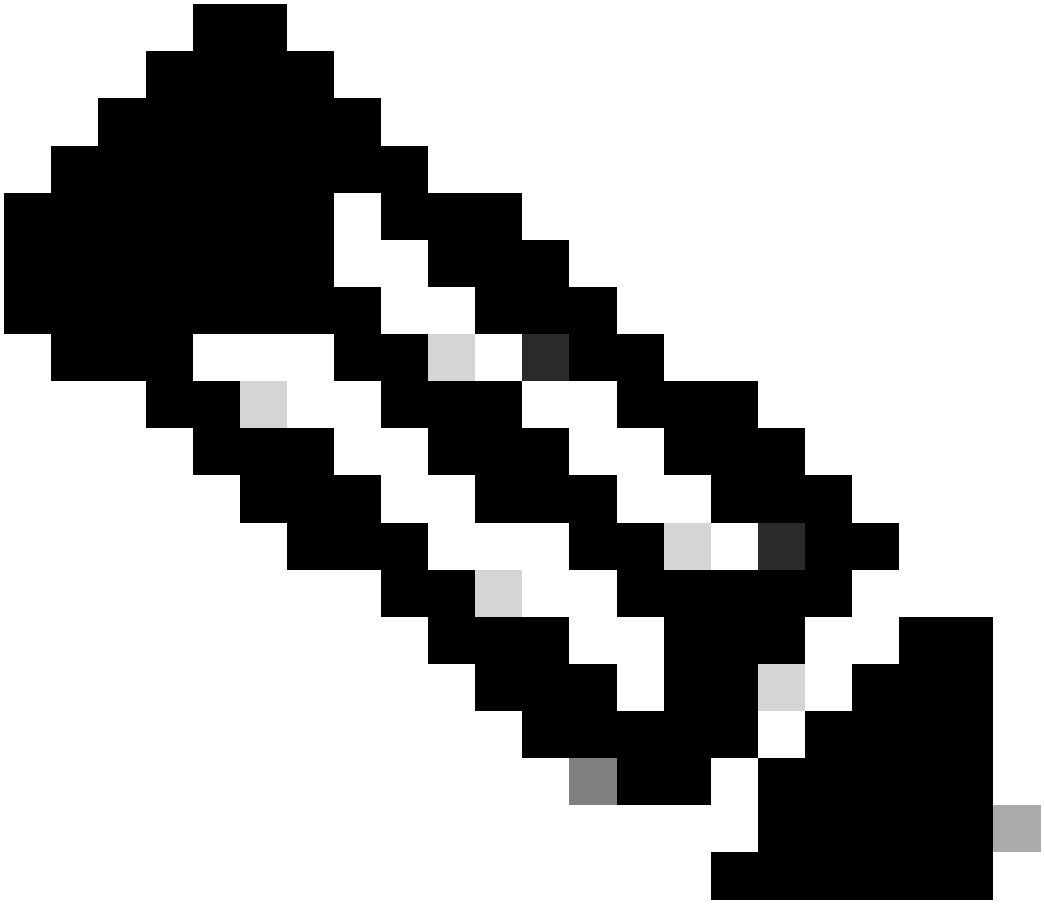
Impossibile modificare il controller con accesso in sola lettura

Queste restrizioni di accesso possono essere verificate anche tramite la CLI del WLC. Questo output mostra un esempio.

```
<#root>

(Cisco Controller) >

?

debug           Manages system debug options.
help            Help
linktest        Perform a link test to a specified MAC address.
logout          Exit this session. Any unsaved changes are lost.
```

```
show            Display switch options and settings.

(Cisco Controller) >config

Incorrect usage.  Use the '?' or <TAB> key to list commands.
```

Come mostrato nell'output di esempio, un'istruzione?alla CLI del controller visualizza un elenco di comandi disponibili per l'utente corrente. Notare anche che il **config** comando non è disponibile nell'output di esempio. Ciò dimostra che un utente di sola lettura non ha il privilegio di eseguire alcuna configurazione sul WLC. Al contrario, un utente in lettura/scrittura non dispone dei privilegi per eseguire le configurazioni sul controller (sia in modalità GUI che CLI).



Nota: anche dopo aver autenticato un utente WLC tramite il server RADIUS, mentre si sfoglia pagina per pagina, il server HTTP[S] esegue comunque l'autenticazione completa del client ogni volta. L'unico motivo per cui non viene richiesta l'autenticazione in ogni

---

pagina è che il browser memorizza nella cache e riproduce le credenziali.

Risoluzione dei problemi

In alcuni casi, quando un controller autentica gli utenti di gestione tramite ACS, l'autenticazione viene completata correttamente (accesso-accettazione) e non viene visualizzato alcun errore di autorizzazione sul controller.*Tuttavia, all'utente viene richiesto nuovamente di eseguire l'autenticazione.*

In questi casi, non è possibile interpretare l'errore e il motivo per cui l'utente non può accedere al WLC con il solo **debug aaa events enable** comando. Viene invece visualizzato un altro prompt per l'autenticazione.

Una delle possibili cause è che ACS non è configurato per trasmettere l'attributo Service-Type per un particolare utente o gruppo, anche se il nome utente e la password sono configurati correttamente su ACS.

L'output del **debug aaa events enable** comando non indica che un utente non dispone degli attributi richiesti (per questo esempio, l'attributo Service-Type) anche se viene inviata una richiesta di **accettazione dell'accesso** dal server AAA. Nell'output del **debug aaa events enable** comando di esempio viene mostrato un esempio.

```
<#root>

(Cisco Controller) >

debug aaa events enable

Mon Aug 13 20:14:33 2011: AuthenticationRequest: 0xa449a8c
Mon Aug 13 20:14:33 2011: Callback.....................................0x8250c40
Mon Aug 13 20:14:33 2011: protocolType.................................0x00020001
Mon Aug 13 20:14:33 2011: proxyState....................1A:00:00:00:00:00-00:00
Mon Aug 13 20:14:33 2011: Packet contains 5 AVPs (not shown)
```

```
Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Successful transmission of
Authentication Packet (id 8) to 172.16.1.1:1812, proxy state
1a:00:00:00:00:00-00:00

Mon Aug 13 20:14:33 2011: ****Enter processIncomingMessages: response code=2

Mon Aug 13 20:14:33 2011: ****Enter processRadiusResponse: response code=2
```

Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Access-Accept received from RADIUS server 172.16.1.1 for mobile 1a:00:00:00:00:00 receiveId = 0

```
Mon Aug 13 20:14:33 2011: AuthorizationResponse: 0x9802520

Mon Aug 13 20:14:33 2011: structureSize.............................28

Mon Aug 13 20:14:33 2011: resultCode.................................0

Mon Aug 13 20:14:33 2011: protocolUsed.............................0x00000001

Mon Aug 13 20:14:33 2011: proxyState......................1A:00:00:00:00:00-00:00

Mon Aug 13 20:14:33 2011: Packet contains 0 AVPs:
```

Nel primo output del **debug aaa events enable** comando di esempio si rileva che Access-Accept è stato ricevuto correttamente dal server RADIUS, ma l'attributo Service-Type non viene passato al WLC. Infatti, l'utente non è configurato con questo attributo su ACS.

È necessario configurare Cisco Secure ACS in modo che restituisca l'attributo Service-Type dopo l'autenticazione dell'utente. Il valore dell'attributo Service-Type deve essere impostato su **Administrative** o **NAS-Prompt** in base ai privilegi utente.

In questo secondo esempio viene mostrato nuovamente l'output del **debug aaa events enable**comando. Tuttavia, questa volta l'attributo Service-Type è impostato su **Administrative** su ACS.

<#root>

(Cisco Controller)>

debug aaa events enable

Mon Aug 13 20:17:02 2011: AuthenticationRequest: 0xa449f1c

Mon Aug 13 20:17:02 2011: Callback.....0x8250c40

Mon Aug 13 20:17:02 2011: protocolType.....0x00020001

Mon Aug 13 20:17:02 2011: proxyState.....1D:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: Packet contains 5 AVPs (not shown)

Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Successful transmission of
Authentication Packet (id 11) to 172.16.1.1:1812, proxy state
1d:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: ****Enter processIncomingMessages: response code=2

Mon Aug 13 20:17:02 2011: ****Enter processRadiusResponse: response code=2

**Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Access-Accept received
from RADIUS server 172.16.1.1 for mobile 1d:00:00:00:00:00 receiveId = 0**

Mon Aug 13 20:17:02 2011: AuthorizationResponse: 0x9802520

Mon Aug 13 20:17:02 2011: structureSize.....100

Mon Aug 13 20:17:02 2011: resultCode.....0

Mon Aug 13 20:17:02 2011: protocolUsed.....0x00000001

Mon Aug 13 20:17:02 2011: proxyState.....1D:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: Packet contains 2 AVPs:

Mon Aug 13 20:17:02 2011: AVP[01] Service-Type.....0x00000006 (6) (4 bytes)

Mon Aug 13 20:17:02 2011: AVP[02] Class.....
CISCOACS:000d1b9f/ac100128/acsserver (36 bytes)

Nell'output dell'esempio precedente è possibile vedere che l'attributo Service-Type viene passato al WLC.

Informazioni correlate

- **Configurazione del controller LAN wireless - Guida alla configurazione**
- **Configurazione delle VLAN sui controller LAN wireless**
- **Configurazione di un server RADIUS e di un WLC per l'assegnazione dinamica della VLAN**
- **Configurazione base dei dispositivi Wireless LAN Controller e Lightweight Access Point**
- **Configurazione delle VLAN del gruppo AP con i controller LAN wireless**
- **Supporto tecnico Cisco e download**

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).