Configurazione Cisco Unified Wireless Network TACACS+

Sommario

Introduzione

Questo documento offre un esempio di configurazione di Terminal Access Controller Access Control System Plus (TACACS+) in un Cisco Wireless LAN Controller (WLC) e in un Cisco

Wireless Control System (WCS) per una rete wireless unificata Cisco. In questo documento vengono inoltre forniti alcuni suggerimenti di base per la risoluzione dei problemi.

TACACS+ è un protocollo client/server che fornisce protezione centralizzata per gli utenti che tentano di ottenere l'accesso di gestione a un router o a un server di accesso alla rete. TACACS+ offre i seguenti servizi AAA:

- Autenticazione degli utenti che tentano di accedere all'apparecchiatura di rete
- Autorizzazione per determinare il livello di accesso che gli utenti devono avere
- Accounting per tenere traccia di tutte le modifiche apportate dall'utente

Per ulteriori informazioni sui servizi AAA e sulla funzionalità TACACS+, consultare il documento sulla configurazione di TACACS+.

per un confronto tra TACACS+ e RADIUS, fare riferimento a Confronto tra TACACS+ e RADIUS.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di come configurare i WLC e i Lightweight Access Point (LAP) per le operazioni di base
- Conoscenza dei metodi LWAPP (Lightweight Access Point Protocol) e di sicurezza wireless
- Conoscenze base RADIUS e TACACS+
- Conoscenze base della configurazione di Cisco ACS

Componenti usati

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

- Cisco Secure ACS per Windows versione 4.0
- Cisco Wireless LAN Controller con versione 4.1.171.0. La funzionalità TACACS+ sui WLC è supportata sulla versione software 4.1.171.0 o successive.
- Cisco Wireless Control System con versione 4.1.83.0. La funzionalità TACACS+ su WCS è supportata dalla versione software 4.1.83.0 o successive.

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.

Implementazione TACACS+ nel controller

Autenticazione

L'autenticazione può essere eseguita usando un database locale, un server RADIUS o TACACS+ che usa un nome utente e una password. L'attuazione non è del tutto modulare. I servizi di autenticazione e autorizzazione sono legati tra loro. Ad esempio, se l'autenticazione viene eseguita utilizzando RADIUS/database locale, l'autorizzazione non viene eseguita con TACACS+. Verrebbero utilizzate le autorizzazioni associate per l'utente nel database locale o RADIUS, ad esempio in sola lettura o in lettura/scrittura, mentre quando si esegue l'autenticazione con TACACS+, l'autorizzazione è associata a TACACS+.

Nei casi in cui sono configurati più database, viene fornita una CLI per dettare la sequenza in cui fare riferimento al database back-end.

Authorization

L'autorizzazione è basata su attività anziché su un'autorizzazione reale basata su comando. Le attività sono associate a varie schede che corrispondono alle sette voci della barra dei menu attualmente presenti nell'interfaccia utente Web. Queste sono le voci della barra dei menu:

- Monitor (Monitora)
- WLAN
- CONTROLLER
- WIRELESS
- SECURITY
- GESTIONE
- COMANDO

Il motivo di questa mappatura si basa sul fatto che la maggior parte dei clienti utilizza l'interfaccia Web per configurare il controller anziché la CLI.

Un ruolo aggiuntivo per la gestione degli amministratori di accesso (LOBBY) è disponibile solo per gli utenti che devono disporre dei privilegi di amministratore di accesso.

L'attività a cui un utente ha diritto è configurata nel server TACACS+ (ACS) utilizzando le coppie attributo-valore (AV) personalizzate. L'utente può essere autorizzato per una o più operazioni. L'autorizzazione minima è SOLO MONITOR e la massima è ALL (autorizzata a eseguire tutte e sette le schede). Se un utente non dispone dei diritti per una determinata operazione, può comunque accedere a tale operazione in modalità di sola lettura. Se l'autenticazione è attivata e il server di autenticazione non è più raggiungibile o non è in grado di autorizzare, l'utente non può accedere al controller.

Nota: per completare correttamente l'autenticazione di gestione di base tramite TACACS+, è necessario configurare i server di autenticazione e autorizzazione sul WLC. La configurazione dell'accounting è facoltativa.

Contabilità

L'accounting viene eseguito ogni volta che viene eseguita correttamente una determinata azione avviata dall'utente. Gli attributi modificati vengono registrati nel server di accounting TACACS+ insieme a quanto segue:

- ID utente della persona che ha apportato la modifica

- Host remoto da cui l'utente ha eseguito l'accesso
- Data e ora di esecuzione del comando
- Livello di autorizzazione dell'utente
- Una stringa che fornisce informazioni sull'azione eseguita e sui valori forniti

Se il server di accounting non è più raggiungibile, l'utente può continuare la sessione.

Nota: i record contabili non vengono generati da Sistema colori Windows nella versione software 4.1 o precedente.

Configurazione TACACS+ nel WLC

Il software WLC versione 4.1.171.0 e successive introduce nuove CLI e modifiche alla GUI del Web per abilitare la funzionalità TACACS+ sul WLC. Le CLI introdotte sono elencate in questa sezione come riferimento. Le modifiche corrispondenti per la GUI Web vengono aggiunte nella scheda Protezione.

in questo documento si presume che la configurazione di base del WLC sia già stata completata.

Per configurare TACACS+ nel controller WLC, completare i seguenti passaggi:

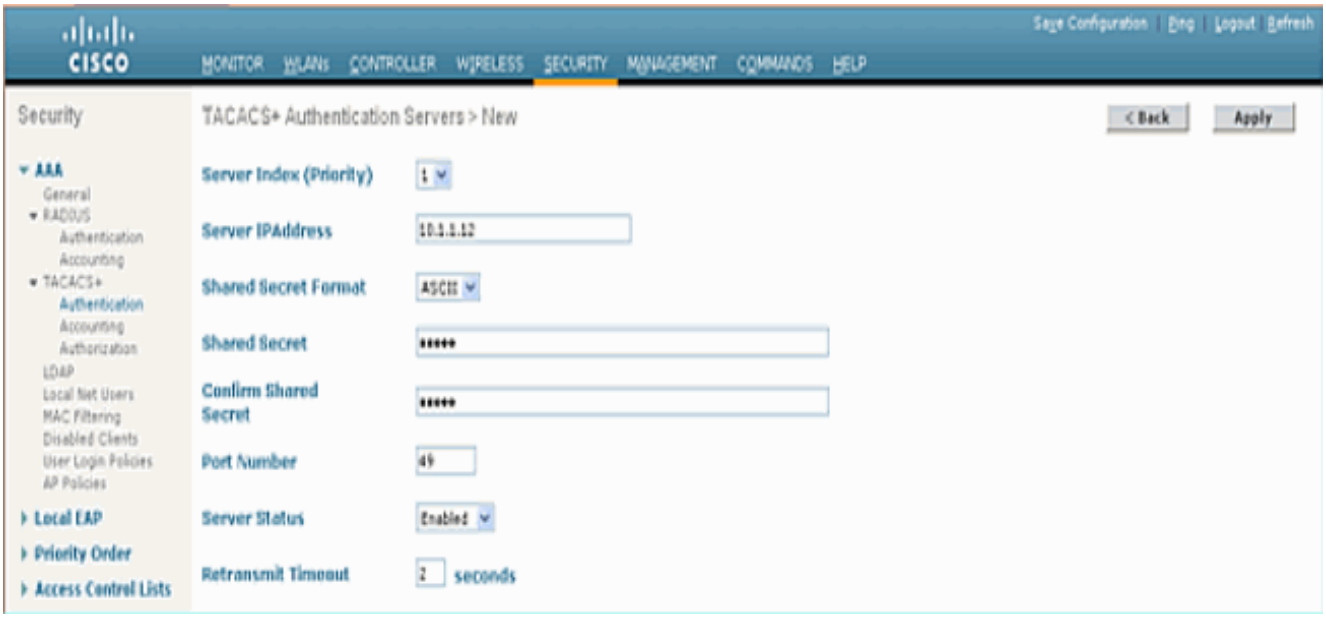
1. Aggiungi server di autenticazione TACACS+
2. Aggiungere un server di autorizzazione TACACS+
3. Aggiungi server di accounting TACACS+
4. Configurazione dell'ordine di autenticazione

Aggiungi server di autenticazione TACACS+

Completare questa procedura per aggiungere un server di autenticazione TACACS+:

1. Usare la GUI e selezionare **Security > TACACS+ > Authentication** (Sicurezza > TACACS+ > Autenticazione).

2. Aggiungere l'indirizzo IP del server TACACS+ e immettere la chiave segreta condivisa. Se necessario, modificare la porta predefinita
TCP/49.



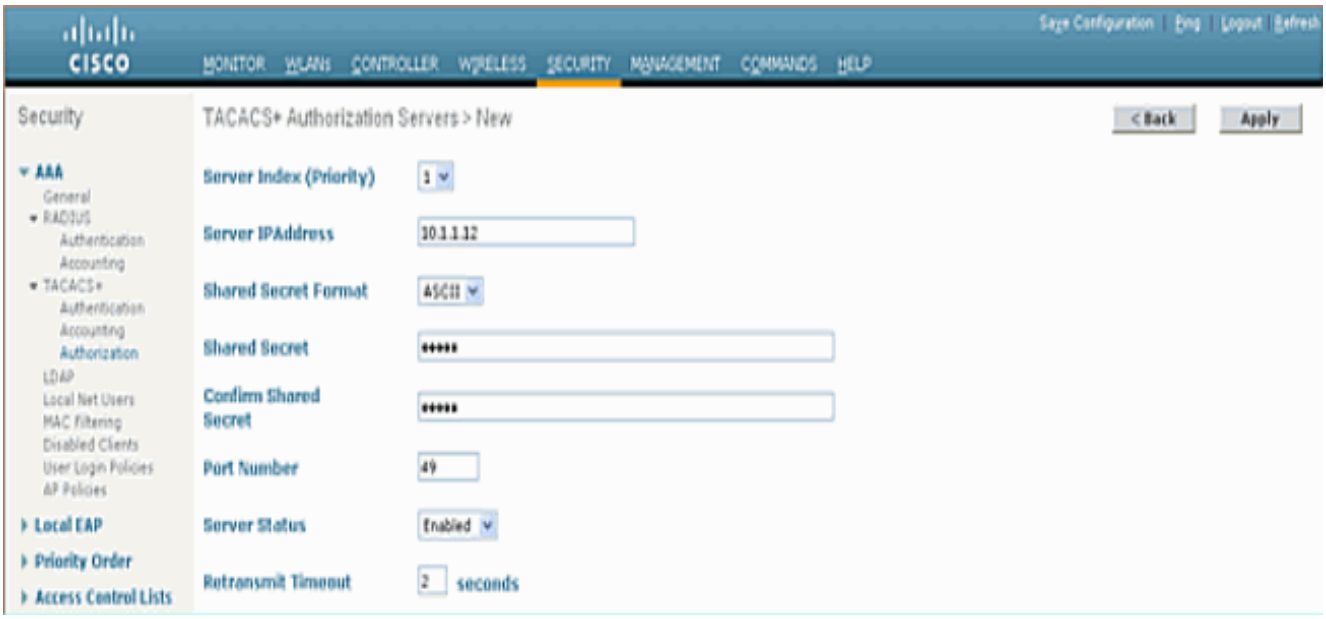
3. Fare clic su **Apply** (Applica).A tale scopo, dalla CLI è possibile usare il comando **config tacacs auth add** *<Indice server> <indirizzo IP> <porta> [ascii/hex]* **<segreto>**:

```
(Cisco Controller) >config tacacs auth add 1 10.1.1.12 49 ascii cisco123
```

Aggiungere un server di autorizzazione TACACS+

Completare questa procedura per aggiungere un server di autorizzazione TACACS+:

1. Dalla GUI, selezionare **Security > TACACS+ > Authorization** (Sicurezza > TACACS+ > Autorizzazione).
2. Aggiungere l'indirizzo IP del server TACACS+ e immettere la chiave segreta condivisa. Se necessario, modificare la porta predefinita TCP/49.



3. Fare clic su **Apply** (Applica).A tale scopo, dalla CLI è possibile usare il comando **config tacacs athr add** *<Indice server> <Indirizzo IP> <porta> [ascii/hex]* **<segreto>**:

```
(Cisco Controller) >config tacacs athr add 1 10.1.1.12 49 ascii cisco123
```

Aggiungi server di accounting TACACS+

Completare questi passaggi per aggiungere un server di accounting TACACS+:

1. Usare la GUI e selezionare **Security > TACACS+ > Accounting** (Sicurezza > TACACS+ > Accounting).
2. Aggiungere l'indirizzo IP del server e immettere la chiave segreta condivisa. Se necessario, modificare la porta predefinita
   TCP/49.

3. Fare clic su **Apply** (Applica).A tale scopo, dalla CLI è possibile usare il comando **config tacacs acct add** *<Indice server> <indirizzo IP> <porta> [ascii/hex]* **<segreto>**:
   ```
   (Cisco Controller) >config tacacs acct add 1 10.1.1.12 49 ascii cisco123
   ```

Configurazione dell'ordine di autenticazione

Questo passaggio spiega come configurare l'ordine di autenticazione AAA quando sono configurati più database. L'ordine di autenticazione può essere **locale e RADIUS**, **locale e TACACS**. La configurazione predefinita del controller per l'ordine di autenticazione è *locale e RADIUS*.

Per configurare l'ordine di autenticazione, completare i seguenti passaggi:

1. Dalla GUI, selezionare **Security > Priority Order > Management User** (Sicurezza > Ordine di priorità > Utente di gestione).
2. Selezionare la priorità di autenticazione.Nell'esempio, è stato selezionato TACACS+.
3. Per eseguire la selezione, fare clic su **Apply**
   (Applica).

A tale scopo, dalla CLI è possibile usare il comando **config aaa auth mgmt** <server1> <server2>:

```
(Cisco Controller) >config aaa auth mgmt tacacs local
```

Verifica configurazione

In questa sezione vengono descritti i comandi utilizzati per verificare la configurazione di TACACS+ sul WLC. Di seguito sono riportati alcuni utili comandi **show** che aiutano a determinare se la configurazione è corretta:

- **show aaa auth**: fornisce informazioni sull'ordine di autenticazione.

```
(Cisco Controller) >show aaa auth
Management authentication server order:
    1..................................... local
    2..................................... Tacacs
```

- **show tacacs summary**: visualizza un riepilogo dei servizi e delle statistiche di TACACS+.

```
(Cisco Controller) >show tacacs summary
Authentication Servers

Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
1    10.1.1.12         49      Enabled   2

Authorization Servers

Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
1    10.1.1.12         49      Enabled   2

Accounting Servers

Idx  Server Address    Port    State     Tout
---  ---------------  ------  --------  ----
1    10.1.1.12         49      Enabled   2
```

- **show tacacs auth stats**: visualizza le statistiche del server di autenticazione TACACS+.

```
(Cisco Controller) >show tacacs auth statistics
Authentication Servers:

Server Index..................................... 1
Server Address..................................... 10.1.1.12
Msg Round Trip Time.............................. 0 (1/100 second)
First Requests................................... 7
Retry Requests................................... 3
Accept Responses................................. 3
```

```
Reject Responses.............................. 0
Error Responses............................... 0
Restart Responses............................. 0
Follow Responses.............................. 0
GetData Responses............................. 0
Encrypt no secret Responses................... 0
Challenge Responses........................... 0
Malformed Msgs................................ 0
Bad Authenticator Msgs........................ 0
Timeout Requests.............................. 12
Unknowntype Msgs.............................. 0
Other Drops................................... 0
```

- **show tacacs athr stats**: visualizza le statistiche del server di autorizzazione TACACS+.

```
(Cisco Controller) >show tacacs athr statistics
Authorization Servers:

Server Index.................................. 1
Server Address................................ 10.1.1.12
Msg Round Trip Time........................... 0 (1/100 second)
First Requests................................ 3
Retry Requests................................ 3
Received Responses............................ 3
Authorization Success......................... 3
Authorization Failure......................... 0
Challenge Responses........................... 0
Malformed Msgs................................ 0
Bad Athrenticator Msgs........................ 0
Timeout Requests.............................. 0
Unknowntype Msgs.............................. 0
Other Drops................................... 0
```

- **show tacacs acct stats**: visualizza le statistiche del server di accounting TACACS+.

```
(Cisco Controller) >show tacacs acct statistics
Accounting Servers:

Server Index.................................. 1
Server Address................................ 10.1.1.12
Msg Round Trip Time........................... 0 (1/100 second)
First Requests................................ 133
Retry Requests................................ 0
Accounting Response........................... 0
Accounting Request Success.................... 0
Accounting Request Failure.................... 0
Malformed Msgs................................ 0
Bad Authenticator Msgs........................ 0
Timeout Requests.............................. 399
Unknowntype Msgs.............................. 0
Other Drops................................... 0
```

Configurazione del server Cisco Secure ACS

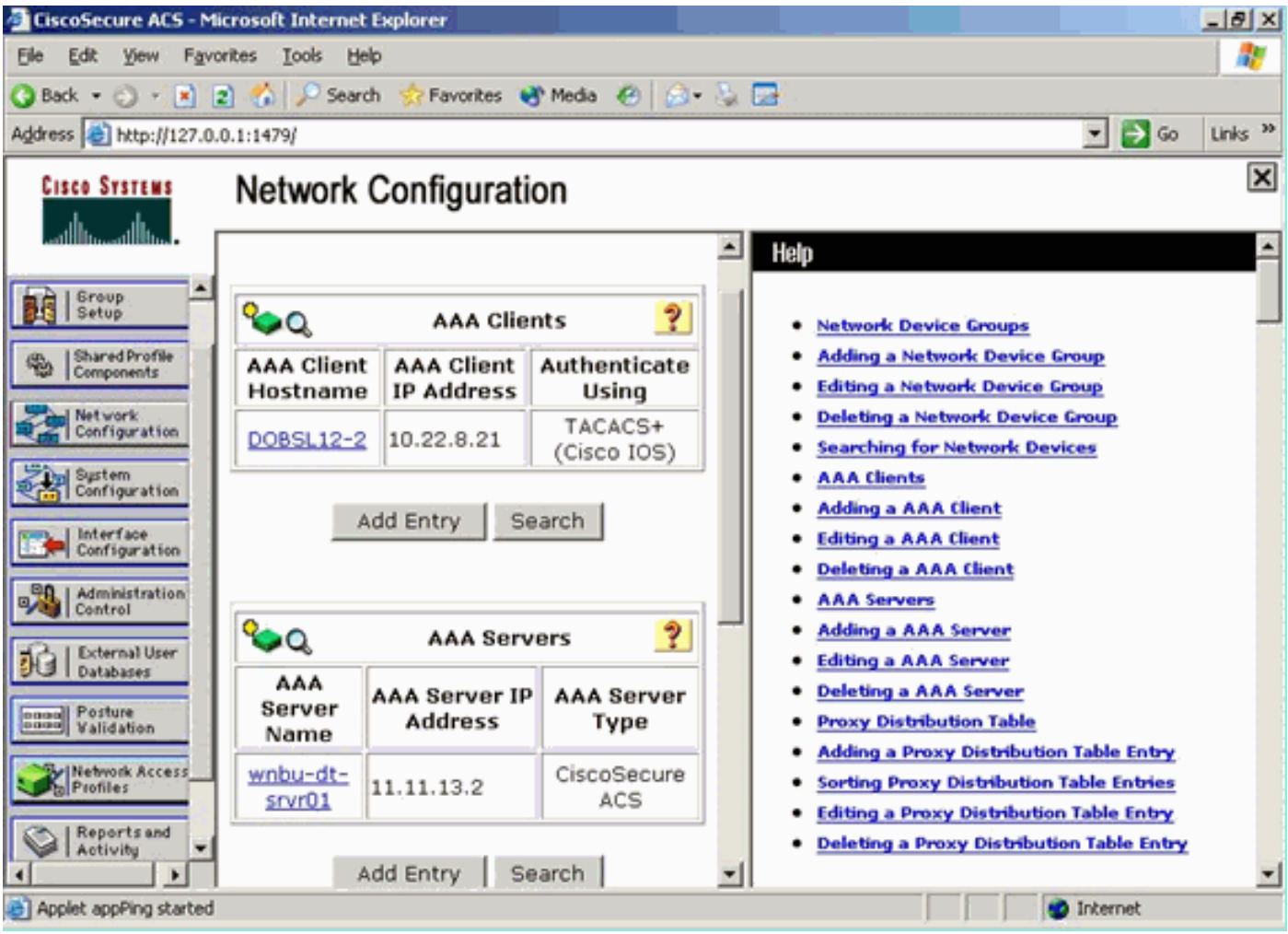
In questa sezione vengono illustrati i passaggi da eseguire sul server TACACS+ ACS per creare servizi e attributi personalizzati e assegnare i ruoli agli utenti o ai gruppi.

In questa sezione non vengono fornite spiegazioni sulla creazione di utenti e gruppi. Si presuppone che gli utenti e i gruppi vengano creati in base alle esigenze. Per informazioni su come creare utenti e gruppi di utenti, consultare la Guida dell'utente di Cisco Secure ACS per Windows Server 4.0.

Configurazione della rete

Eseguire questo passaggio:

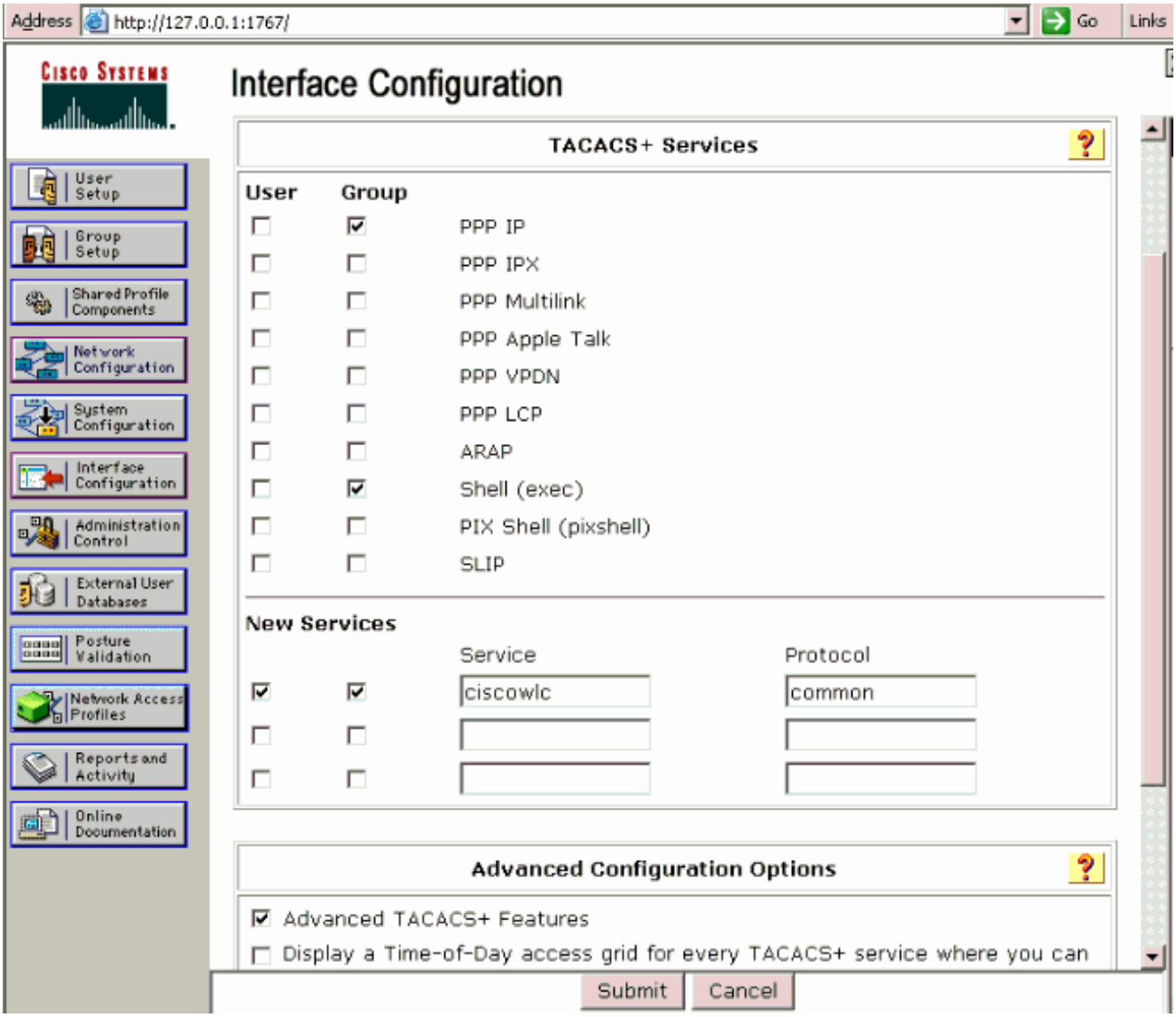
Aggiungere l'indirizzo IP di gestione del controller come client AAA con il meccanismo di autenticazione TACACS+ (Cisco IOS).



Configurazione interfaccia

Attenersi alla seguente procedura:

1. Nel menu Interface Configuration, selezionare il collegamento **TACACS+** (Cisco IOS).
2. Abilitare i **nuovi servizi**.
3. Selezionare le caselle di controllo **Utente** e **Gruppo**.
4. Immettere **ciscowlc** for Service e **common** for Protocol.
5. Abilitare le **funzionalità avanzate** **TACACS+**.

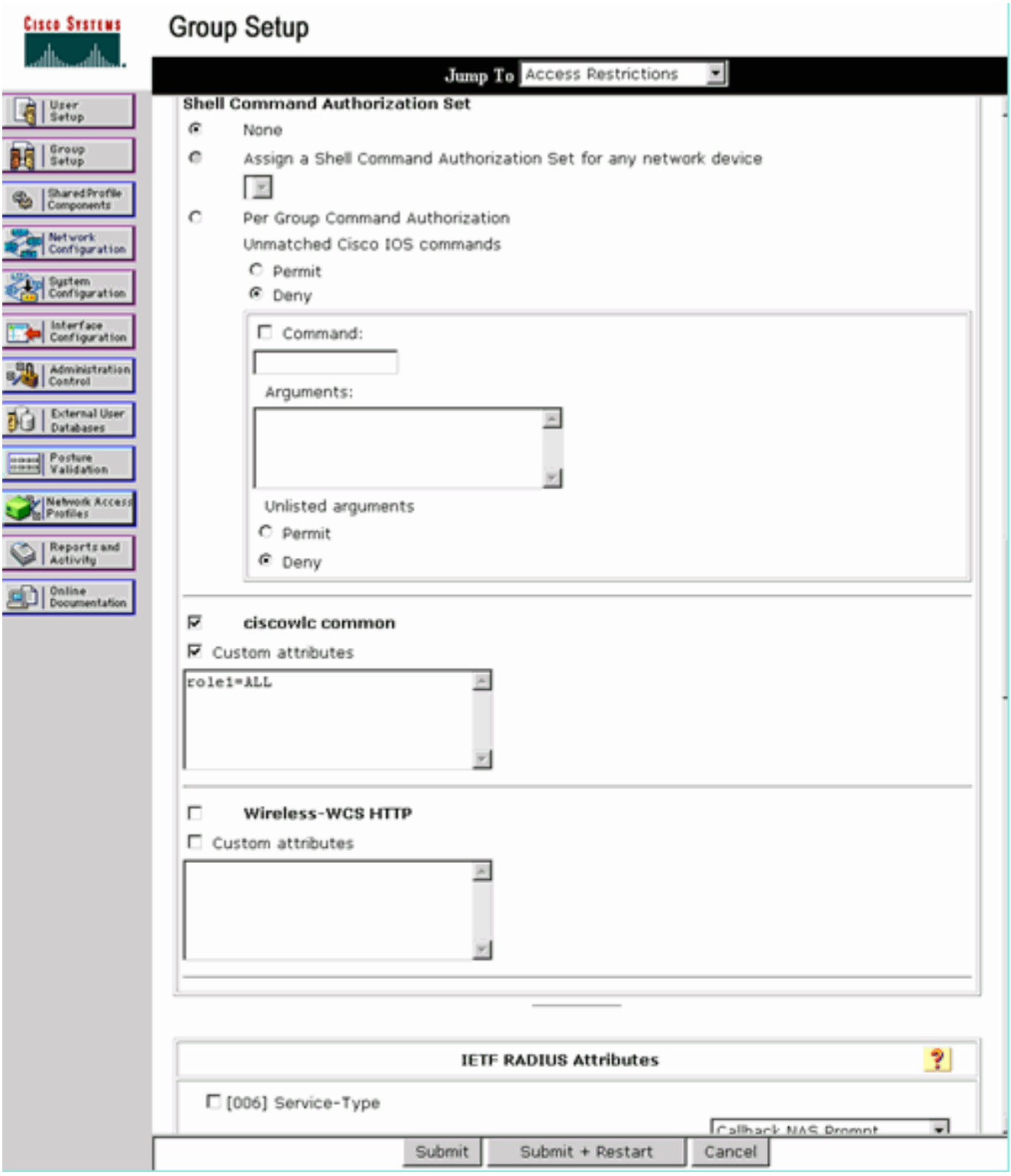


6. Per applicare le modifiche, fare clic su **Submit** (Invia).

Configurazione utente/gruppo

Attenersi alla seguente procedura:

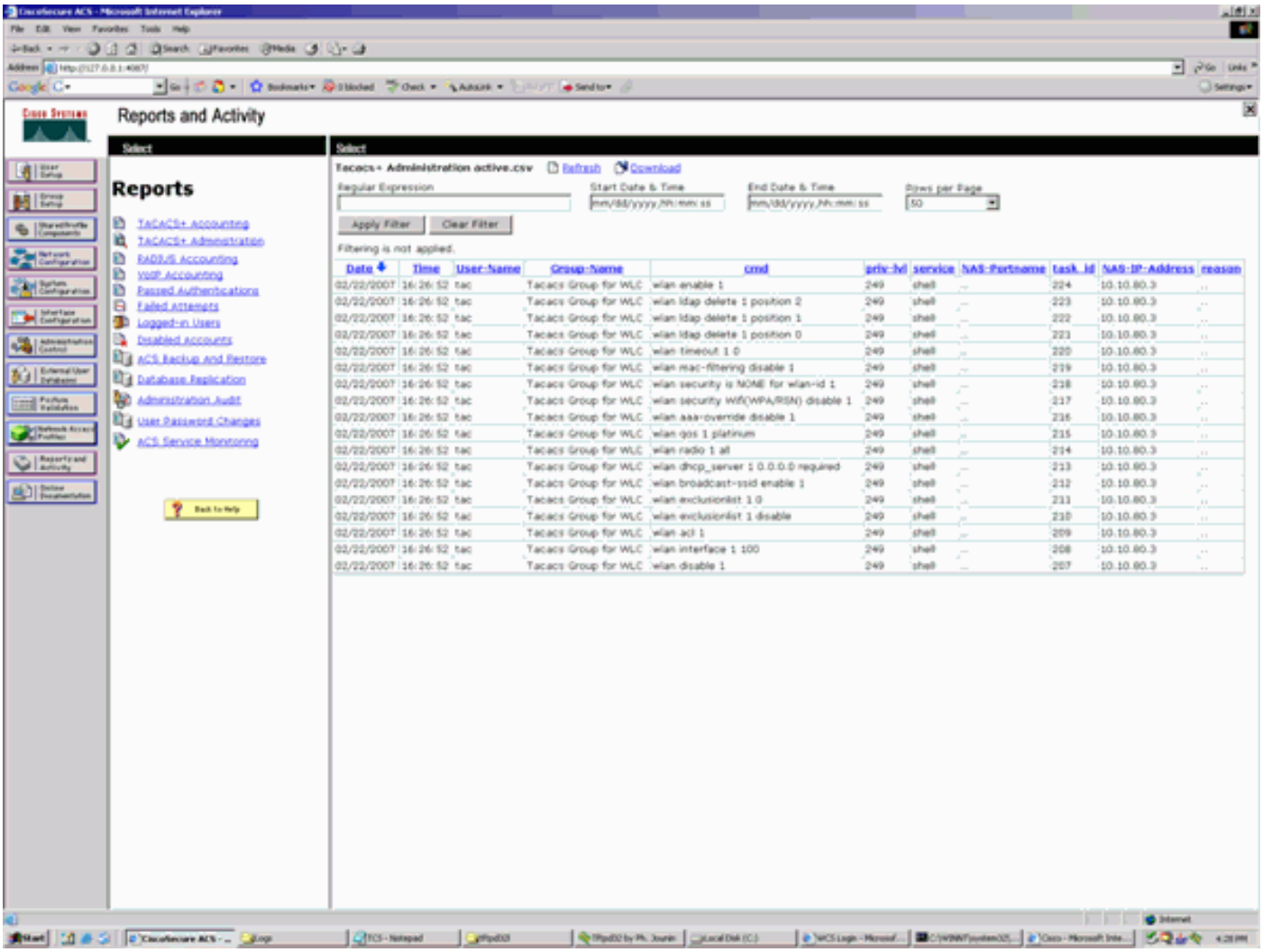
1. Selezionare un utente/gruppo creato in precedenza.
2. Andare a **Impostazioni TACACS+**.
3. Selezionare la casella di controllo corrispondente al servizio *ciscowlc* creato nella sezione Configurazione interfaccia.
4. Selezionare la casella di controllo **Attributi personalizzati**.



5. Nella casella di testo sotto Attributi personalizzati, immettere questo testo se l'utente creato deve accedere solo a WLAN, SECURITY e CONTROLLER: **role1=WLAN role2=SECURITY role3=CONTROLLER**.Se l'utente deve accedere solo alla scheda SECURITY, immettere il testo seguente: **role1=SICUREZZA**.Il ruolo corrisponde alle sette voci della barra dei menu nell'interfaccia utente Web del controller. Le voci della barra dei menu sono MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT e COMMAND.
6. Immettere il ruolo necessario a un utente per ruolo1, ruolo2 e così via. Se un utente necessita di tutti i ruoli, deve essere utilizzata la parola chiave **ALL**. Per il ruolo di amministratore della sala di attesa, utilizzare la parola chiave **LOBBY**.

Record di accounting in Cisco Secure ACS

I record contabili TACACS+ dal WLC sono disponibili in Cisco Secure ACS nella pagina TACACS+ Administration of Reports and Activity:

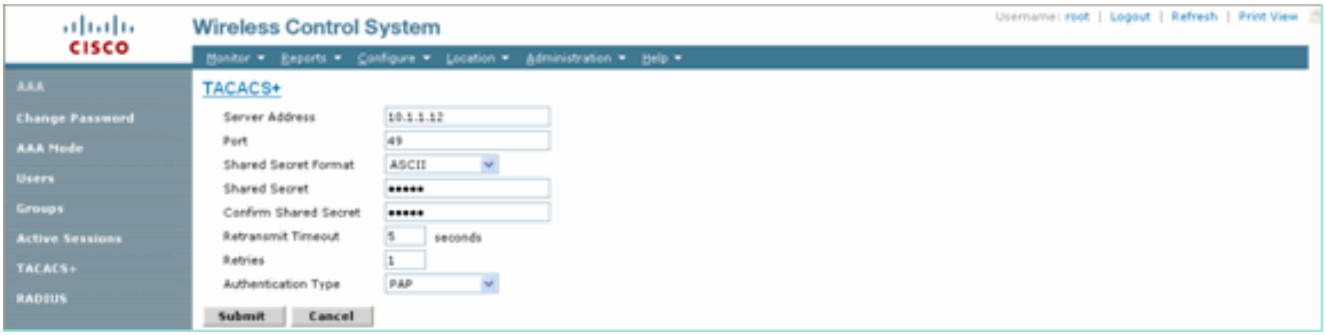


Configurazione TACACS+ nel sistema WCS

Attenersi alla seguente procedura:

1. Dalla GUI, accedere al sistema WCS con l'account root.
2. Aggiungere il server TACACS+. Selezionare **Amministrazione > AAA > TACACS+ > Aggiungi server TACACS+**.

3. Aggiungere i dettagli del server TACACS+, ad esempio l'indirizzo IP, il numero di porta (il valore predefinito è 49) e la chiave segreta condivisa.



4. Abilitare l'autenticazione TACACS+ per l'amministrazione in WCS. Selezionare **Administration > AAA > AAA Mode > Select TACACS+**.

Sistema colori Windows con domini virtuali

Dominio virtuale è una nuova funzionalità introdotta con WCS versione 5.1. Un dominio virtuale WCS è costituito da un insieme di dispositivi e mappe e limita la visualizzazione dell'utente alle informazioni relative a tali dispositivi e mappe. Tramite un dominio virtuale, un amministratore può garantire che gli utenti possano visualizzare solo i dispositivi e le mappe di cui sono responsabili. Inoltre, grazie ai filtri del dominio virtuale, gli utenti possono configurare, visualizzare gli allarmi e generare report solo per la parte di rete loro assegnata. L'amministratore specifica un set di domini virtuali consentiti per ogni utente. Solo uno di questi può essere attivo per l'utente al login. L'utente può modificare il dominio virtuale corrente selezionando un dominio virtuale consentito diverso dal menu a discesa Dominio virtuale nella parte superiore dello schermo. Tutti i report, gli allarmi e le altre funzionalità sono ora filtrati in base al dominio virtuale.

Se nel sistema è definito un solo dominio virtuale (radice) e l'utente non ha domini virtuali nei campi degli attributi personalizzati nel server TACACS+/RADIUS, all'utente viene assegnato il dominio virtuale radice per impostazione predefinita.

Se esistono più domini virtuali e l'utente non dispone di attributi specificati, l'accesso dell'utente verrà bloccato. Per consentire all'utente di accedere, gli attributi personalizzati del dominio virtuale devono essere esportati nel server Radius/TACACS+.

La finestra Attributi personalizzati dominio virtuale consente di indicare i dati specifici del protocollo appropriati per ogni dominio virtuale. Il pulsante Export (Esporta) sulla barra laterale Gerarchia domini virtuali (Virtual Domain Hierarchy) consente di preformattare gli attributi RADIUS e TACACS+ del dominio virtuale. È possibile copiare e incollare questi attributi nel server ACS. In questo modo è possibile copiare solo i domini virtuali applicabili nella schermata del server ACS e garantire che gli utenti abbiano accesso solo a questi domini virtuali.

Per applicare gli attributi RADIUS e TACACS+ preformattati al server ACS, completare la procedura descritta nella sezione Attributi RADIUS e TACACS+ del dominio virtuale.

Configurazione di Cisco Secure ACS per l'utilizzo di WCS

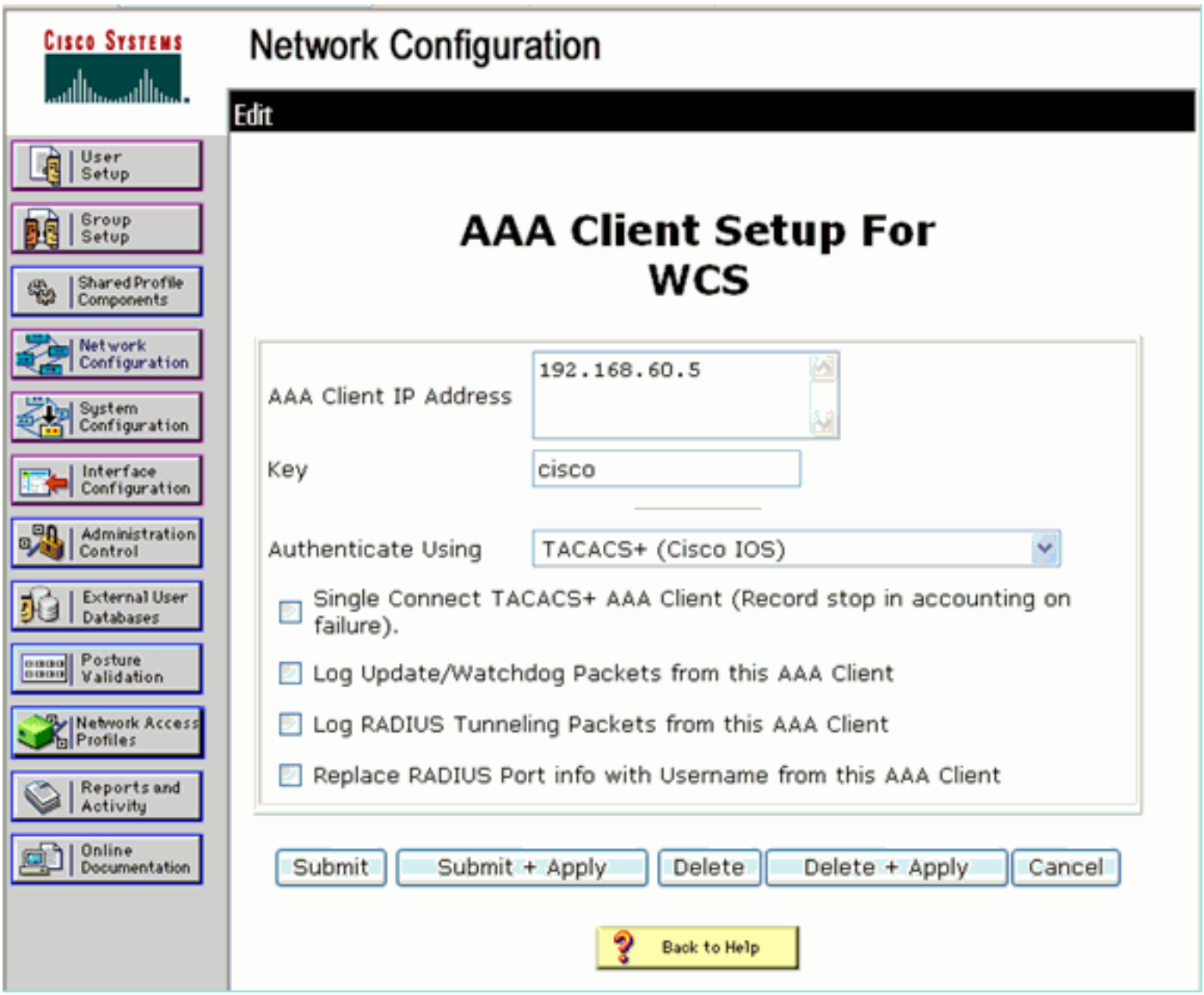
In questa sezione vengono illustrati i passaggi da eseguire sul server TACACS+ ACS per creare servizi e attributi personalizzati e assegnare i ruoli agli utenti o ai gruppi.

In questa sezione non vengono fornite spiegazioni sulla creazione di utenti e gruppi. Si presuppone che gli utenti e i gruppi vengano creati in base alle esigenze.

Configurazione della rete

Eseguire questo passaggio:

Aggiungere l'indirizzo IP di WCS come client AAA con il meccanismo di autenticazione TACACS+ (Cisco IOS).

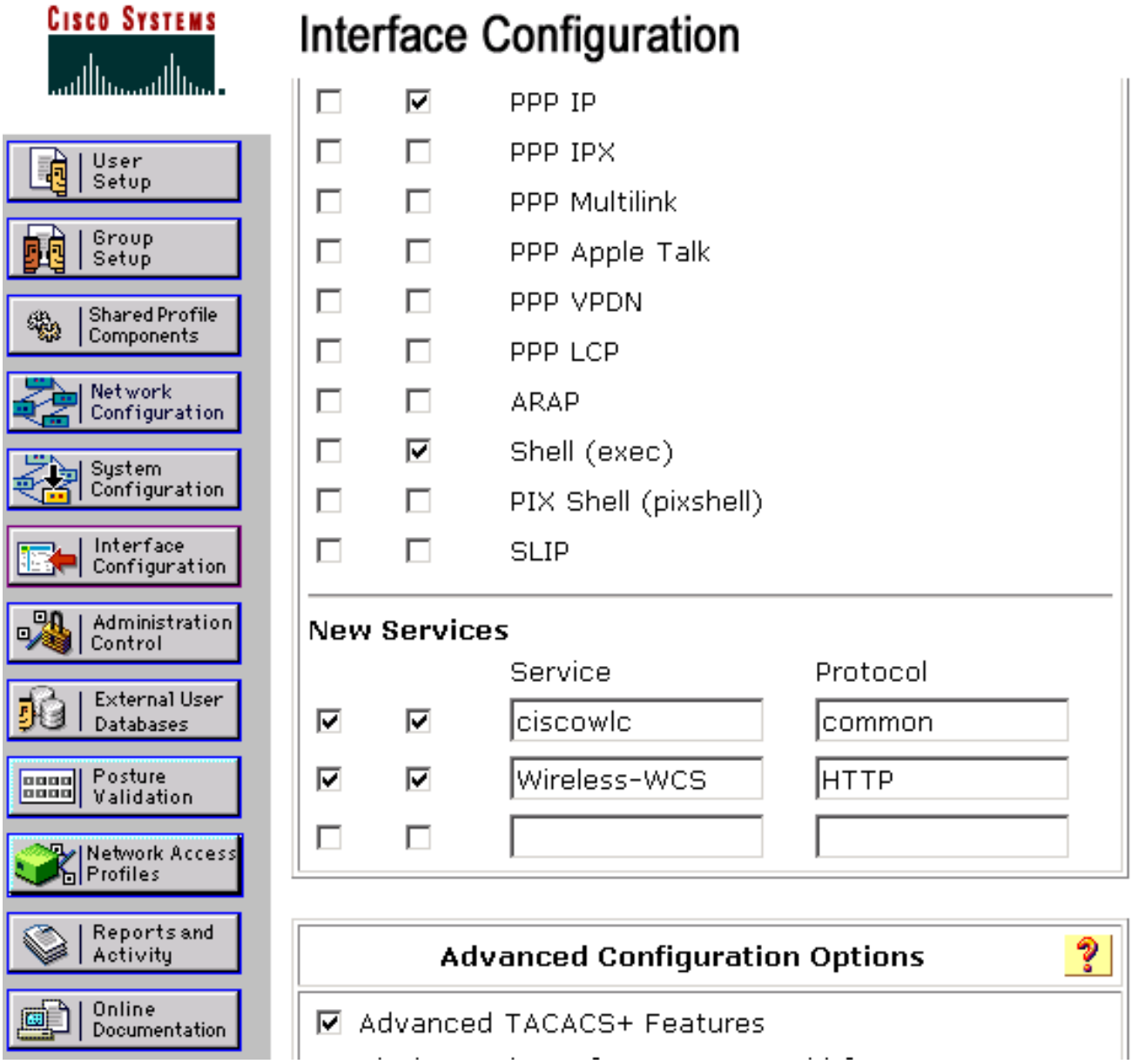


Configurazione interfaccia

Attenersi alla seguente procedura:

1. Nel menu Interface Configuration, selezionare il collegamento **TACACS+** (Cisco IOS).

2. Abilitare i **nuovi servizi**.
3. Selezionare le caselle di controllo **Utente** e **Gruppo**.
4. Immettere **Wireless-WCS** per Service e **HTTP** per Protocol.**Nota:** HTTP deve essere in formato CAPS.
5. Abilitare le **funzionalità avanzate TACACS+**.

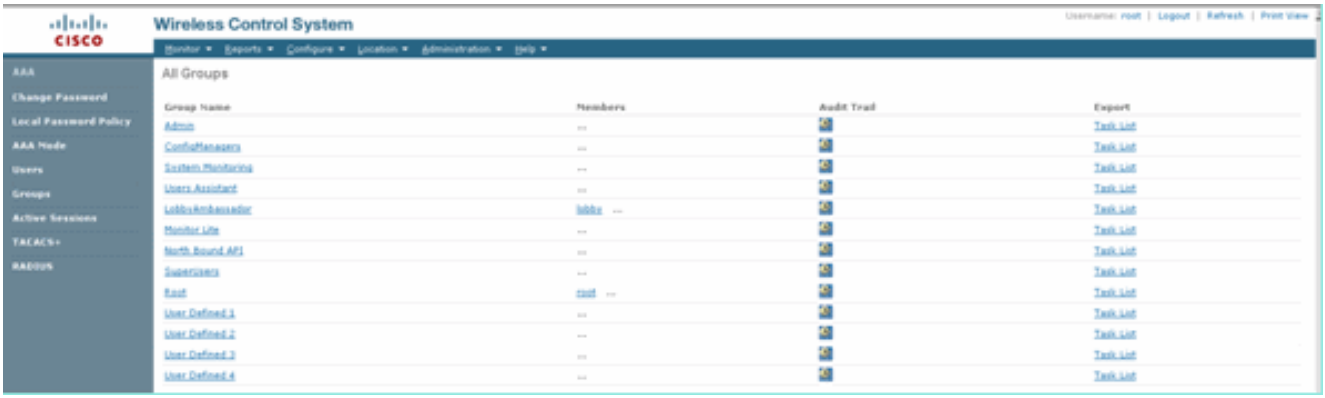


6. Per applicare le modifiche, fare clic su **Submit** (Invia).

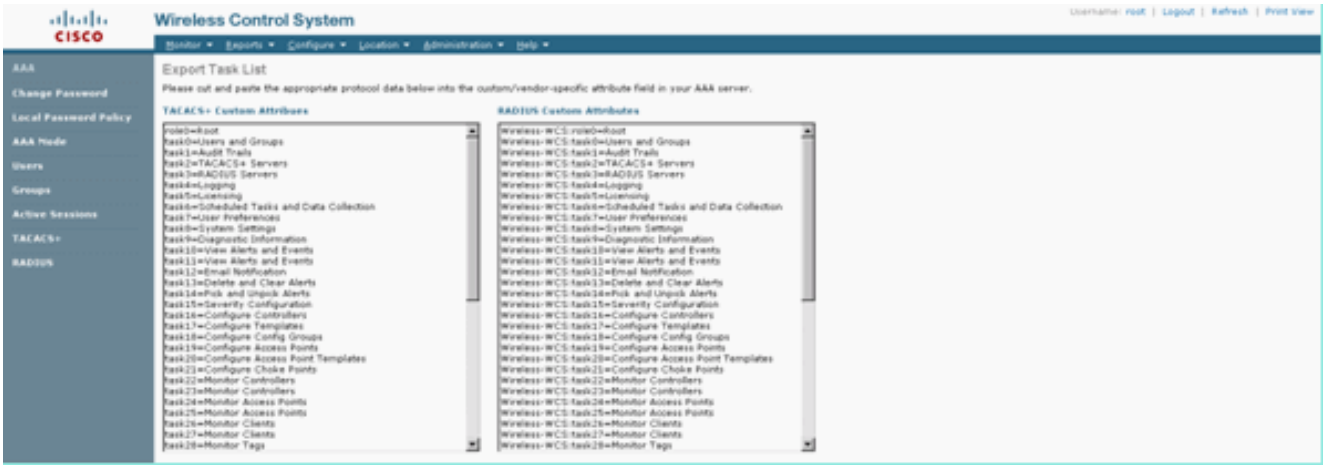
Configurazione utente/gruppo

Attenersi alla seguente procedura:

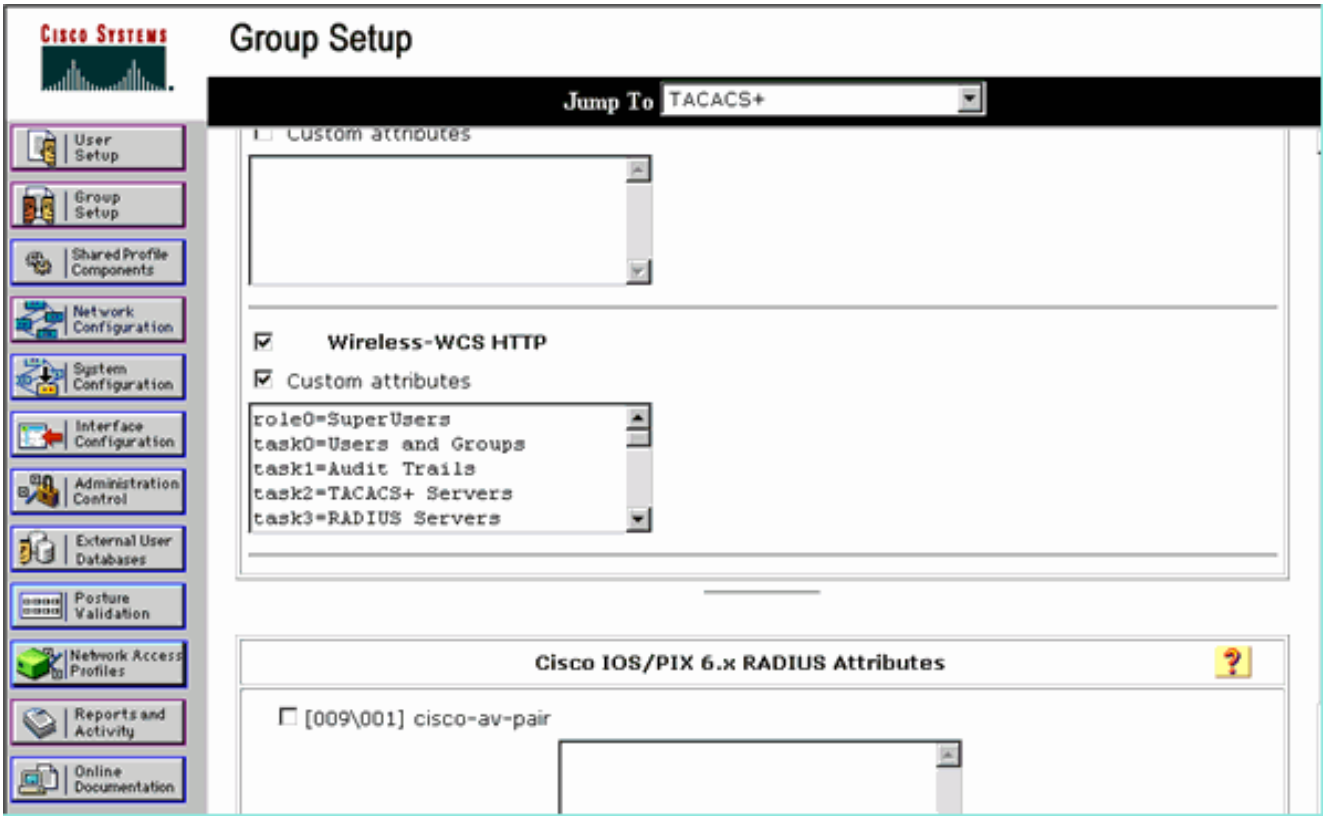
1. Nell'interfaccia utente di WCS, selezionare **Amministrazione > AAA > Gruppi** per selezionare uno dei gruppi di utenti preconfigurati, ad esempio SuperUsers in WCS.



2. Selezionare l'Elenco task per i gruppi di utenti preconfigurati e copiare e incollare nell'ACS.



3. Selezionare un utente/gruppo creato in precedenza e andare a **Impostazioni TACACS+**.
4. Nell'interfaccia utente di ACS selezionare la casella di controllo corrispondente al servizio Wireless-WCS creato in precedenza.
5. Nell'interfaccia utente di ACS, selezionare la casella **Attributi personalizzati**.
6. Nella casella di testo sotto Attributi personalizzati, immettere queste informazioni sul ruolo e sull'attività copiate da Sistema colori Windows. Ad esempio, immettere l'elenco delle attività consentite dagli utenti
privilegiati.



7. Quindi, accedere al Sistema colori Windows con il nome utente/password appena creato nel server ACS.

Debug

Debug da WLC per role1=ALL

```
(Cisco Controller) >debug aaa tacacs enable

(Cisco Controller) >Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=2 session_id=5eaa857e
length=16 encrypted=0
Wed Feb 28 17:36:37 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:36:37 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:36:37 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=4 session_id=5eaa857e
length=6 encrypted=0
Wed Feb 28 17:36:37 2007: tplus_make_author_request() from tplus_authen_passed returns rc=0
Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:36:37 2007: author response body: status=1 arg_cnt=1 msg_len=0 data_len=0
Wed Feb 28 17:36:37 2007: arg[0] = [9][role1=ALL]
Wed Feb 28 17:36:37 2007: User has the following mgmtRole fffffff8
```

Debug da WLC per più ruoli

```
(Cisco Controller) >debug aaa tacacs enable

Wed Feb 28 17:59:33 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=2
session_id=b561ad88 length=16 encrypted=0
Wed Feb 28 17:59:34 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:59:34 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:59:34 2007: processTplusAuthResponse: Continue auth transaction
```

```
Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=4 session_id=b561ad88
length=6 encrypted=0
Wed Feb 28 17:59:34 2007: tplus_make_author_request() from tplus_authen_passed
returns rc=0
Wed Feb 28 17:59:34 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:59:34 2007: author response body: status=1 arg_cnt=4 msg_len=0 data_len=0
Wed Feb 28 17:59:34 2007: arg[0] = [11][role1=WLAN]
Wed Feb 28 17:59:34 2007: arg[1] = [16][role2=CONTROLLER]
Wed Feb 28 17:59:34 2007: arg[2] = [14][role3=SECURITY]
Wed Feb 28 17:59:34 2007: arg[3] = [14][role4=COMMANDS]
Wed Feb 28 17:59:34 2007: User has the following mgmtRole 150
```

Debug da un WLC per errore di autorizzazione

```
(Cisco Controller) >debug aaa tacacs enable

Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=2 session_id=89c553a1
length=16 encrypted=0
Wed Feb 28 17:53:04 2007: TPLUS_AUTHEN_STATUS_GETPASS
Wed Feb 28 17:53:04 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:53:04 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=4 session_id=89c553a1
length=6 encrypted=0
Wed Feb 28 17:53:04 2007: tplus_make_author_request() from tplus_authen_passed
returns rc=0
Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: author response body: status=16 arg_cnt=0 msg_len=0 data_len=0
Wed Feb 28 17:53:04 2007:User has the following mgmtRole 0
Wed Feb 28 17:53:04 2007: Tplus authorization for tac failed status=16
```

Informazioni correlate

- Esempio di configurazione di Cisco Wireless LAN Controller (WLC) e Cisco ACS 5.x (TACACS+) per l'autenticazione Web
- Configurazione di TACACS+
- Come configurare l'autenticazione e l'autorizzazione TACACS per gli utenti amministratori e non amministratori in ACS 5.1
- Confronto tra TACACS+ e RADIUS
- Documentazione e supporto tecnico – Cisco Systems