Lock-and-Key: Elenchi di accesso dinamico

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Convenzioni](#)
[Considerazioni sullo spoofing](#)
[Prestazioni](#)
[Quando utilizzare l'accesso Lock-and-Key](#)
[Operazione di accesso Lock-and-Key](#)
[Esempio di configurazione e risoluzione dei problemi](#)
[Esempio di rete](#)
[Uso di TACACS+](#)
[Utilizzo di RADIUS](#)
[Informazioni correlate](#)

Introduzione

L'accesso Lock-and-Key consente di impostare elenchi di accesso dinamici che concedono l'accesso per utente a un host di origine/destinazione specifico tramite un processo di autenticazione utente. L'accesso degli utenti è consentito dinamicamente attraverso un firewall di Cisco IOS®, senza compromettere le restrizioni di sicurezza.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. In questo caso, l'ambiente lab è costituito da un router 2620 con software Cisco IOS® versione 12.3(1). 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.

Considerazioni sullo spoofing

L'accesso tramite lock-and-key consente a un evento esterno di posizionare un'apertura nel firewall Cisco IOS. Dopo questa apertura, il router è esposto allo spoofing dell'indirizzo di origine. Per evitare questo problema, fornire il supporto della crittografia usando la crittografia IP con autenticazione o crittografia.

Lo spoofing è un problema con tutti gli elenchi degli accessi esistenti. L'accesso Lock-and-Key non risolve questo problema.

Poiché l'accesso con blocco e chiave introduce un potenziale percorso attraverso il firewall di rete, è necessario considerare l'accesso dinamico. Un altro host, che falsifica l'indirizzo autenticato, ottiene l'accesso dietro il firewall. L'accesso dinamico consente a un host non autorizzato, che falsifica l'indirizzo autenticato, di accedere attraverso il firewall. L'accesso tramite Lock-and-Key non causa problemi di spoofing degli indirizzi. Il problema è qui identificato solo come un problema per l'utente.

Prestazioni

Le prestazioni sono influenzate da queste due situazioni.

- Ogni elenco accessi dinamico forza la ricostruzione di un elenco accessi sul motore di commutazione del silicio (SSE, Silicon Switching Engine). In questo modo, il percorso di commutazione SSE si rallenta momentaneamente.
- Gli elenchi degli accessi dinamici richiedono una funzione di timeout di inattività (anche se il timeout è impostato su predefinito). Pertanto, gli elenchi degli accessi dinamici non possono essere commutati SSE. Queste voci vengono gestite nel percorso di commutazione rapida del protocollo.

Controllare le configurazioni del router di confine. Gli utenti remoti creano voci dell'elenco accessi sul router di confine. L'elenco degli accessi cresce e si riduce in modo dinamico. Le voci vengono rimosse dinamicamente dall'elenco dopo la scadenza del timeout di inattività o del timeout massimo. Gli elenchi degli accessi di grandi dimensioni compromettono le prestazioni di switching dei pacchetti.

Quando utilizzare l'accesso Lock-and-Key

Di seguito sono elencati due esempi di utilizzo dell'accesso Lock-and-Key:

- Quando si desidera che un host remoto sia in grado di accedere a un host nella rete interna tramite Internet. L'accesso Lock-and-Key limita l'accesso al di fuori del firewall su un singolo host o in rete.
- Quando si desidera che un sottoinsieme di host in una rete acceda a un host in una rete remota protetto da un firewall. Con l'accesso lock-and-key, è possibile consentire l'accesso

solo a un set di host desiderato tramite la relativa autenticazione su un server TACACS+ o RADIUS.

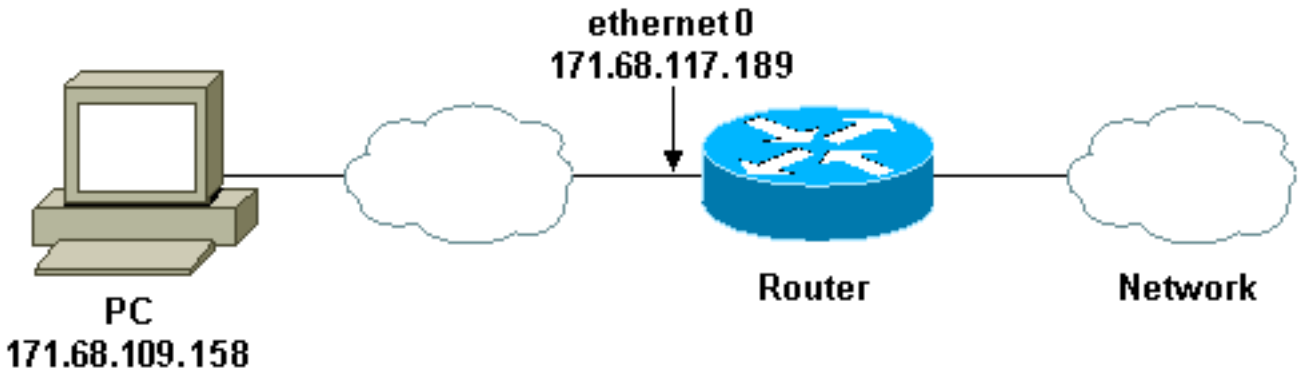
Operazione di accesso Lock-and-Key

In questo processo viene descritta l'operazione di accesso Lock and Key.

1. Un utente apre una sessione Telnet su un router di confine configurato per l'accesso con blocco e chiave.
2. Il software Cisco IOS riceve il pacchetto Telnet. Esegue un processo di autenticazione utente. L'utente deve passare l'autenticazione prima di poter accedere. Il processo di autenticazione viene eseguito dal router o da un server di accesso centrale, ad esempio un server TACACS+ o RADIUS.

Esempio di configurazione e risoluzione dei problemi

Esempio di rete



Cisco consiglia di utilizzare un server TACACS+ per il processo di query di autenticazione. TACACS+ offre servizi di autenticazione, autorizzazione e accounting. Fornisce inoltre il supporto del protocollo, le specifiche del protocollo e un database di sicurezza centralizzato.

Èpossibile autenticare l'utente sul router o con un server TACACS+ o RADIUS.

Nota: Questi comandi sono globali se non diversamente indicato.

Sul router, è necessario un **nome utente** per l'utente per l'autenticazione locale.

```
username test password test
```

La presenza di **login local** sulle linee vty causa l'uso di questo nome utente.

```
line vty 0 4
login local
```

Se l'utente non è attendibile per l'esecuzione del comando **access-enable**, è possibile eseguire una delle due operazioni seguenti:

- Associare il timeout all'utente per singolo utente.

```
username test autocommand access-enable host
timeout 10
```

o

- Impostare lo stesso timeout per tutti gli utenti che utilizzano Telnet.

```
line vty 0 4
login local
autocommand access-enable host timeout 10
```

Nota: il valore **10** nella sintassi è il timeout di *inattività* dell'elenco degli accessi. Viene ignorato dal timeout assoluto nell'elenco degli accessi dinamici.

Definire un elenco degli accessi estesi che viene applicato quando un utente (qualsiasi utente) accede al router e viene emesso il comando **access-enable**. Il tempo massimo assoluto per questo "foro" nel filtro è impostato su 15 minuti. Dopo 15 minuti, il foro si chiude indipendentemente dal fatto che lo si utilizzi o meno. Il nome **testlist** deve esistere ma non è significativo. Limitare le reti a cui l'utente ha accesso configurando l'indirizzo di origine o di destinazione (in questo caso l'utente non è limitato).

```
access-list 120 dynamic testlist timeout 15 permit ip any any
```

Definire l'elenco degli accessi necessario per bloccare tutto tranne la possibilità di accedere al router in modalità Telnet (per aprire un foro, è necessario che l'utente si connetta al router in modalità Telnet). L'indirizzo IP qui è l'indirizzo IP Ethernet del router.

```
access-list 120 permit tcp any host 171.68.117.189 eq telnet
```

Alla fine c'è una **negazione** implicita (non immessa qui).

Applica l'elenco degli accessi all'interfaccia da cui provengono gli utenti.

```
interface ethernet1
       ip access-group 120 in
```

Hai finito.

Ecco l'aspetto del filtro sul router in questo momento:

```
Router#show access-lists
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

Gli utenti che ottengono l'accesso alla rete interna non sono in grado di visualizzare nulla finché

non si collegano in modalità Telnet al router.

Nota: il valore **10** rappresenta il timeout di *inattività* dell'elenco degli accessi. Viene ignorato dal timeout assoluto nell'elenco degli accessi dinamici.

```
%telnet 2514A
Trying 171.68.117.189 ...
Connected to 2514A.network.com.
Escape character is '^]'.

User Access Verification

Username: test
Password: test

Connection closed by foreign host.
```

Il filtro ha questo aspetto.

```
Router#show access-lists
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.158 any log (time left 394)
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

Esiste un buco nel filtro per questo utente in base all'indirizzo IP di origine. Quando qualcun altro fa questo, si vedono *due buchi*.

```
Router#show ip access-lists 120
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.64 any log
       permit ip host 171.68.109.158 any log
    20 permit tcp any host 171.68.117.189 eq telnet (288 matches)
```

Questi utenti possono accedere completamente a qualsiasi indirizzo IP di destinazione dal proprio indirizzo IP di *origine*.

Uso di TACACS+

Configurazione di TACACS+

Configurare un server TACACS+ per forzare l'autenticazione e l'autorizzazione sul server TACACS+ in modo da utilizzare TACACS+, come mostrato nell'output:

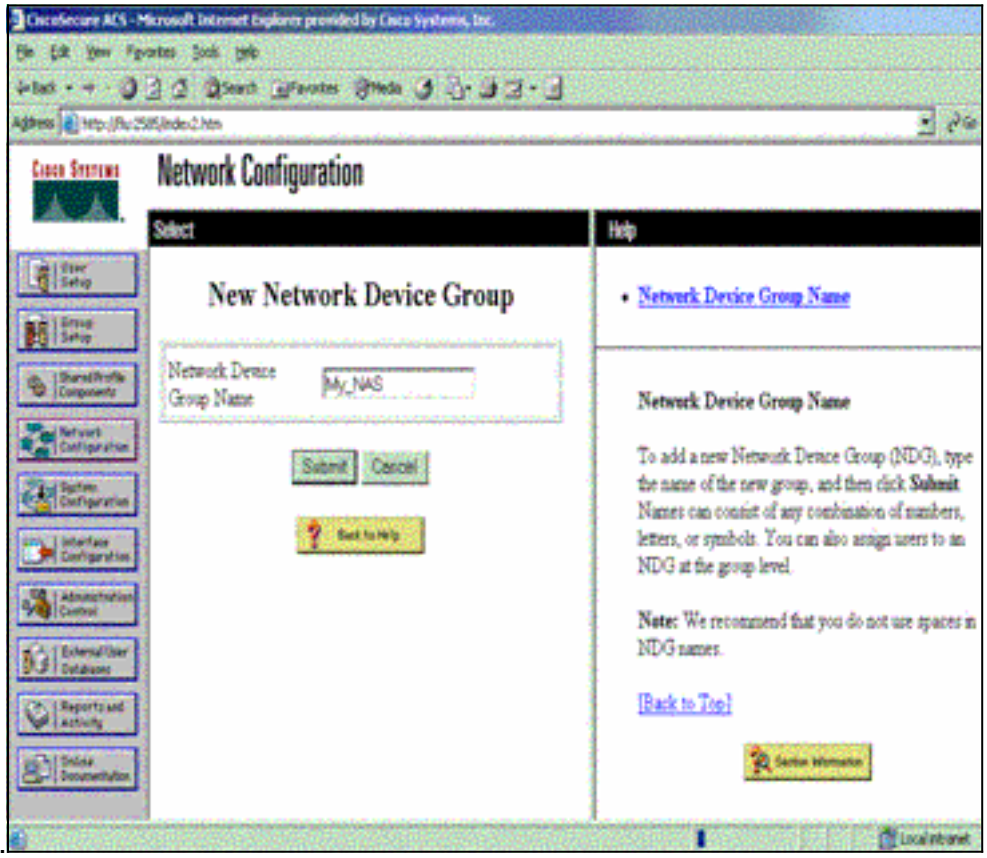
```
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+
tacacs-server host 10.48.66.53 key cisco123
```

Completare la procedura seguente per configurare TACACS+ su Cisco Secure ACS per Windows:

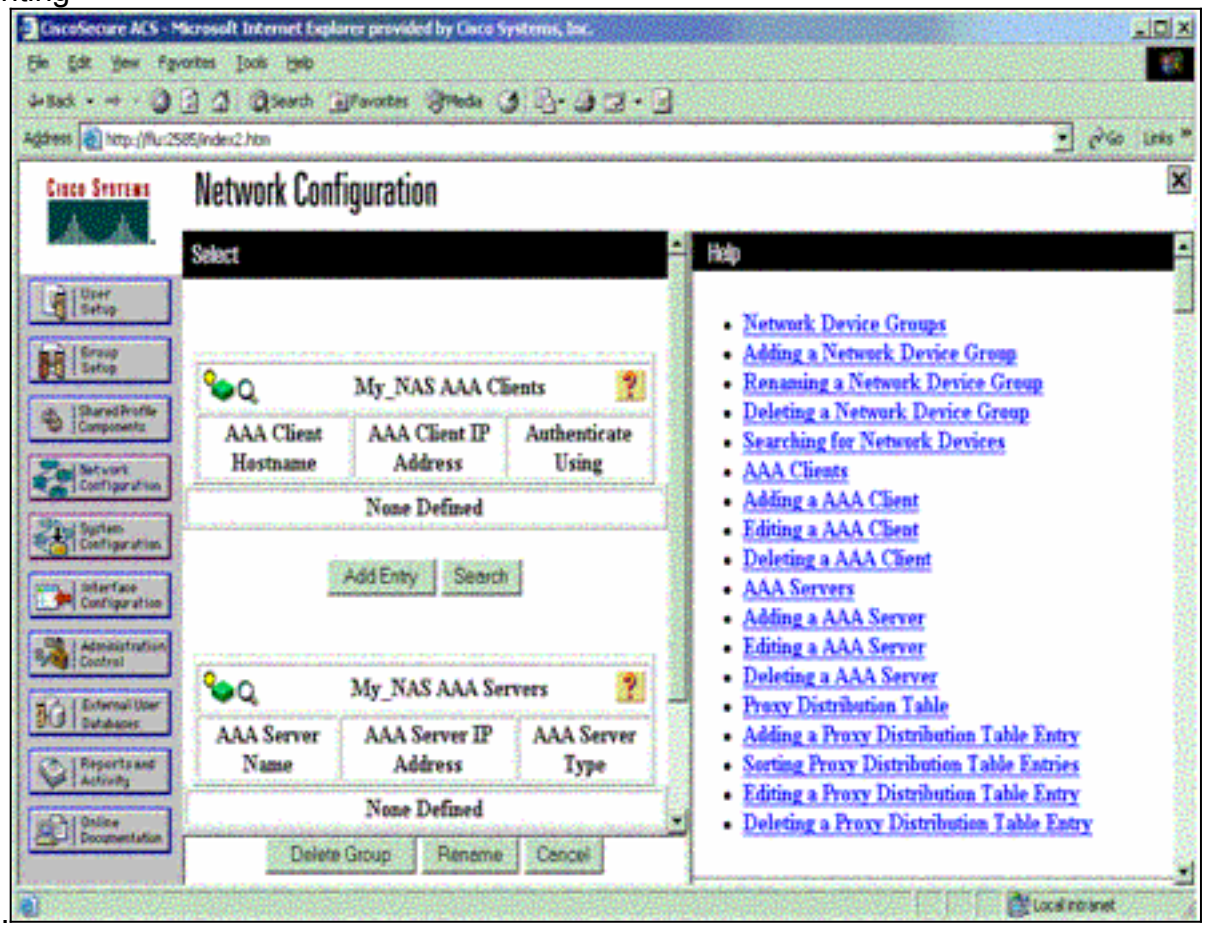
1. Aprire un browser Web. Immettere l'indirizzo del server ACS nel formato **http://*<indirizzo_IP o nome_DNS>*:2002**. In questo esempio viene utilizzata una porta predefinita, ovvero 2002.

Accedere come admin.

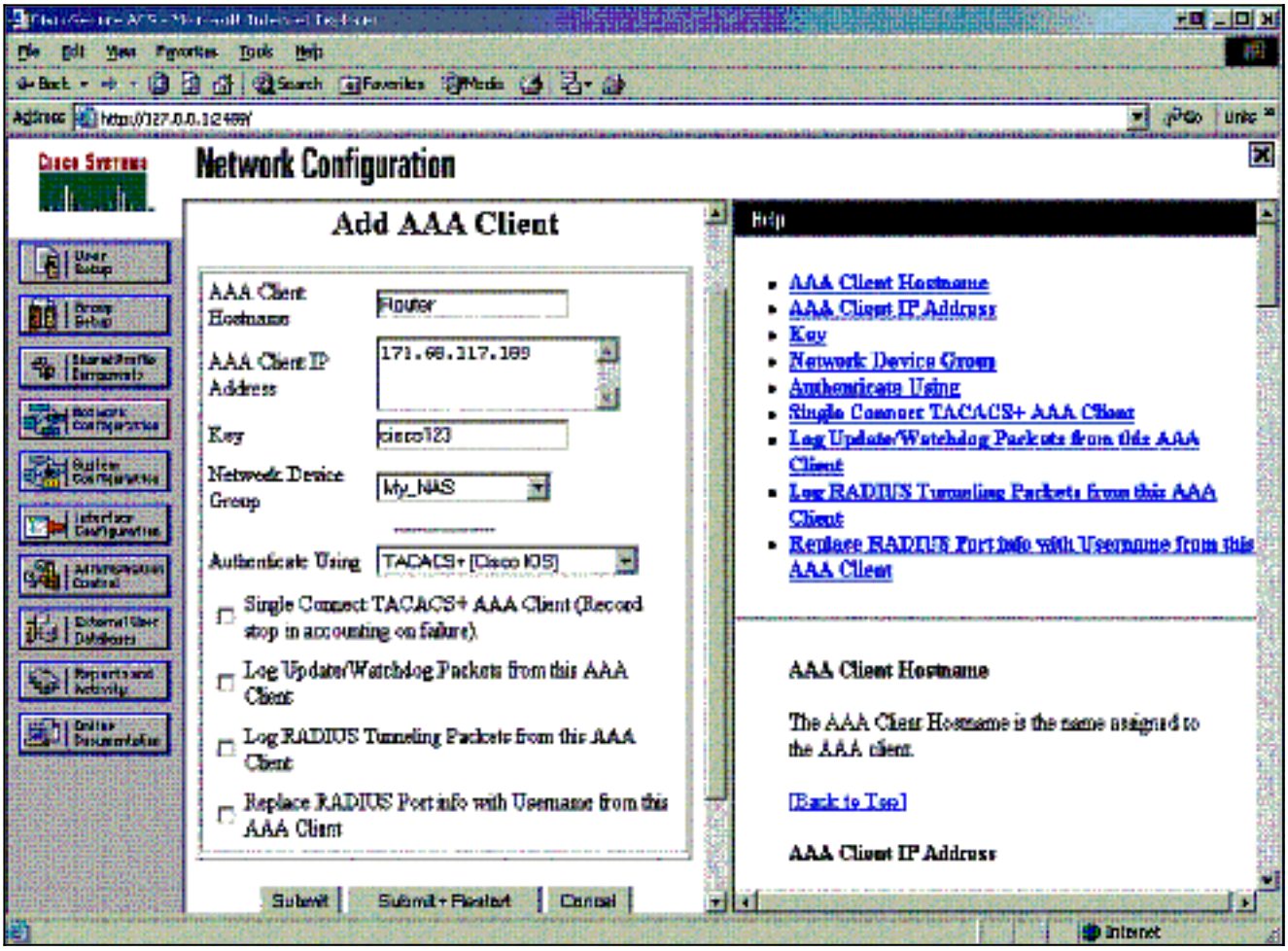
2. Fare clic su **Configurazione di rete**. Fare clic su **Aggiungi voce** per creare un gruppo di dispositivi di rete contenente i server di accesso alla rete (NAS). Immettere un nome per il gruppo e fare clic su **Invia**.



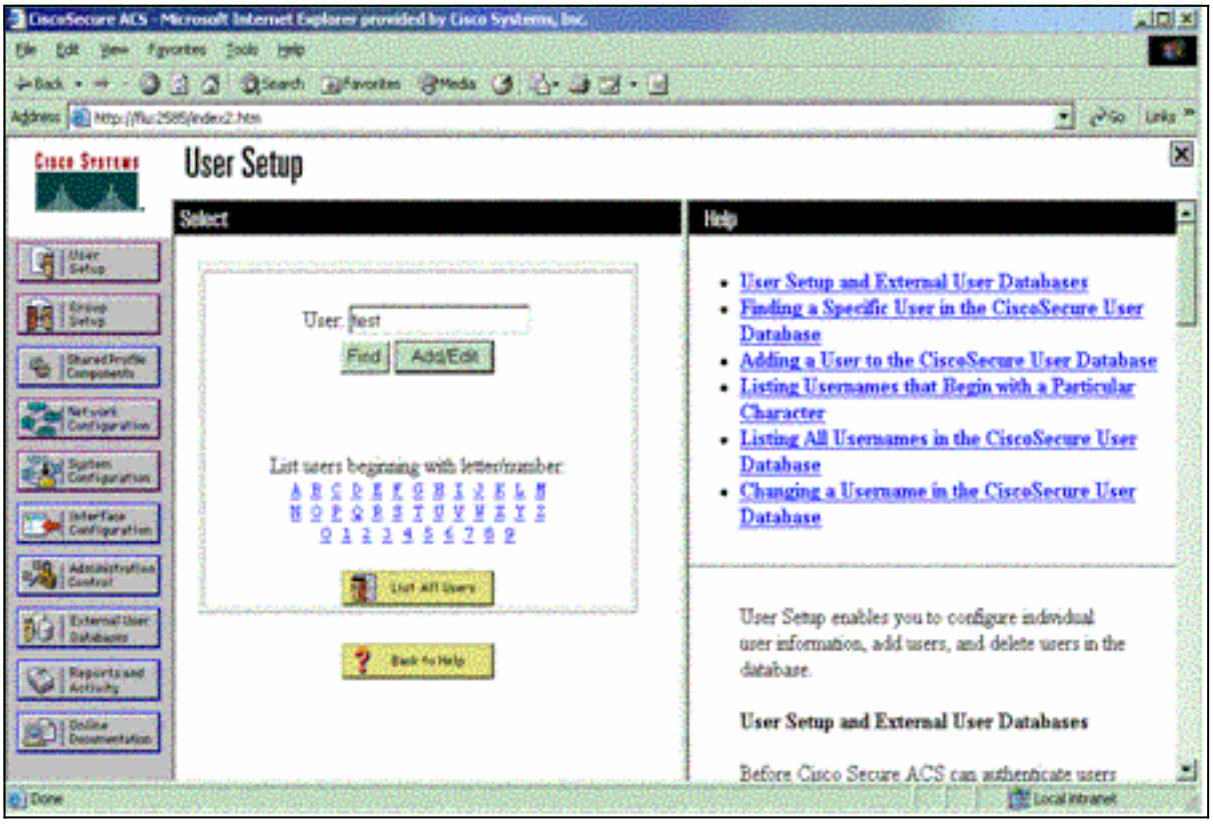
3. Fare clic su **Aggiungi voce** per aggiungere un client di autenticazione, autorizzazione e accounting (AAA).



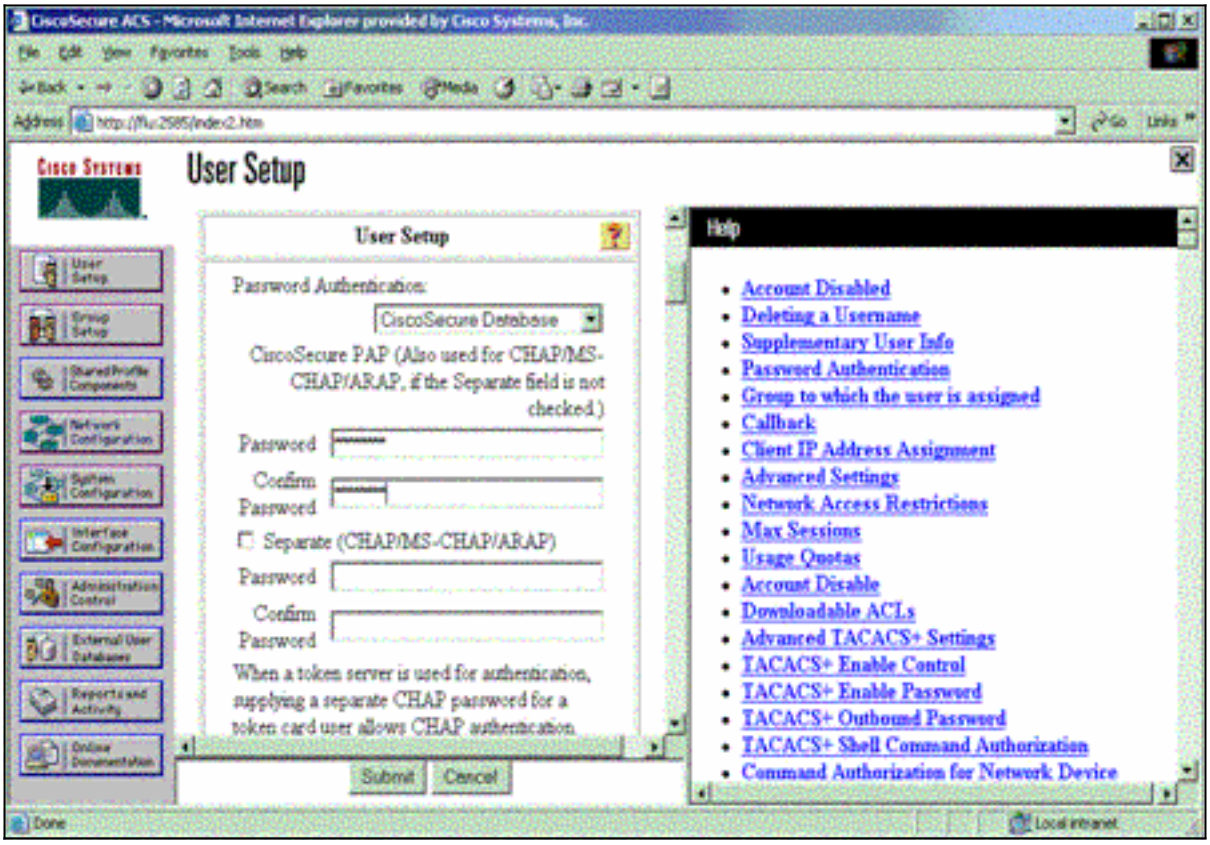
4. Immettere il nome host, l'indirizzo IP e la chiave utilizzata per crittografare la comunicazione tra il server AAA e il server NAS. Selezionare **TACACS+ (Cisco IOS)** come metodo di autenticazione. Al termine, fare clic su **Invia +Riavvia** per applicare le modifiche.



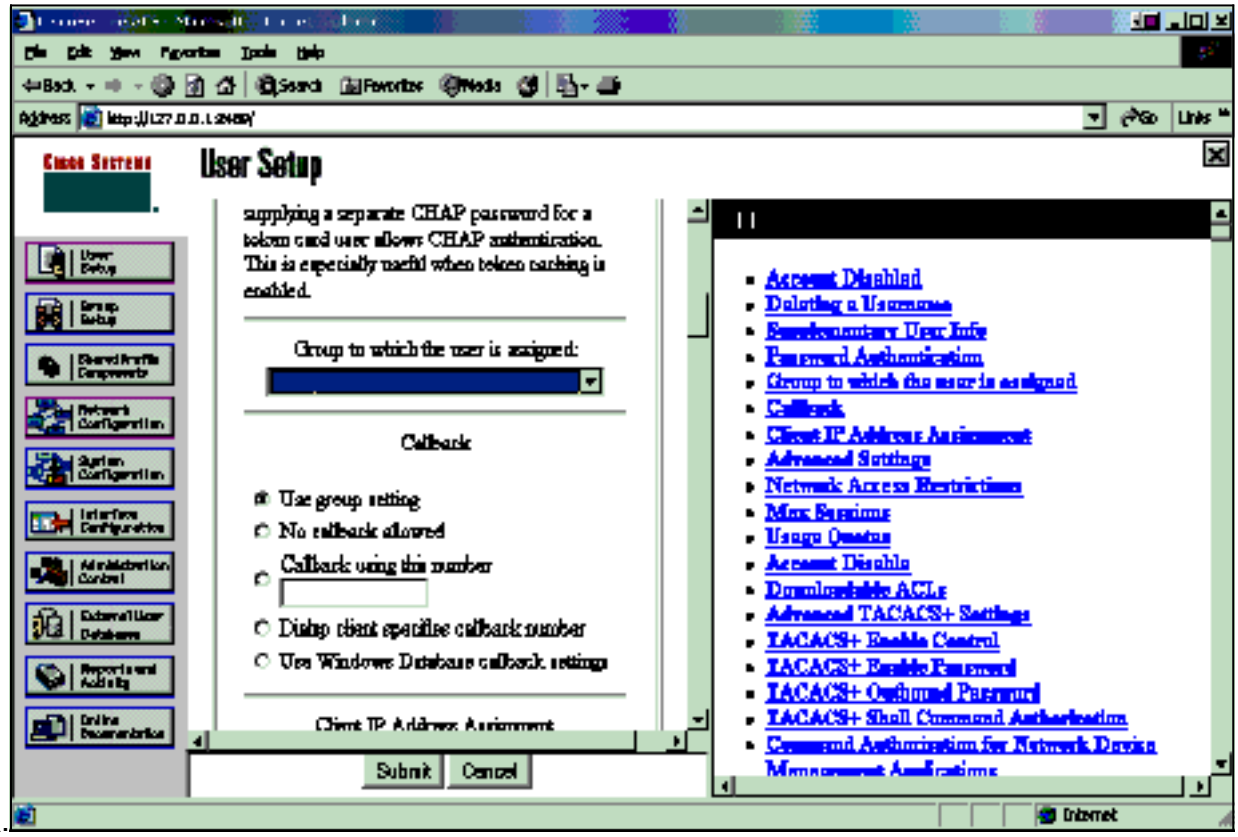
5. Fare clic su **User Setup**, immettere un ID utente e fare clic su **Add/Edit**.



6. Scegliere un database per autenticare l'utente. In questo esempio, l'utente è "test" e per l'autenticazione viene utilizzato il database interno del server ACS. Immettere una password per l'utente e
confermarla.

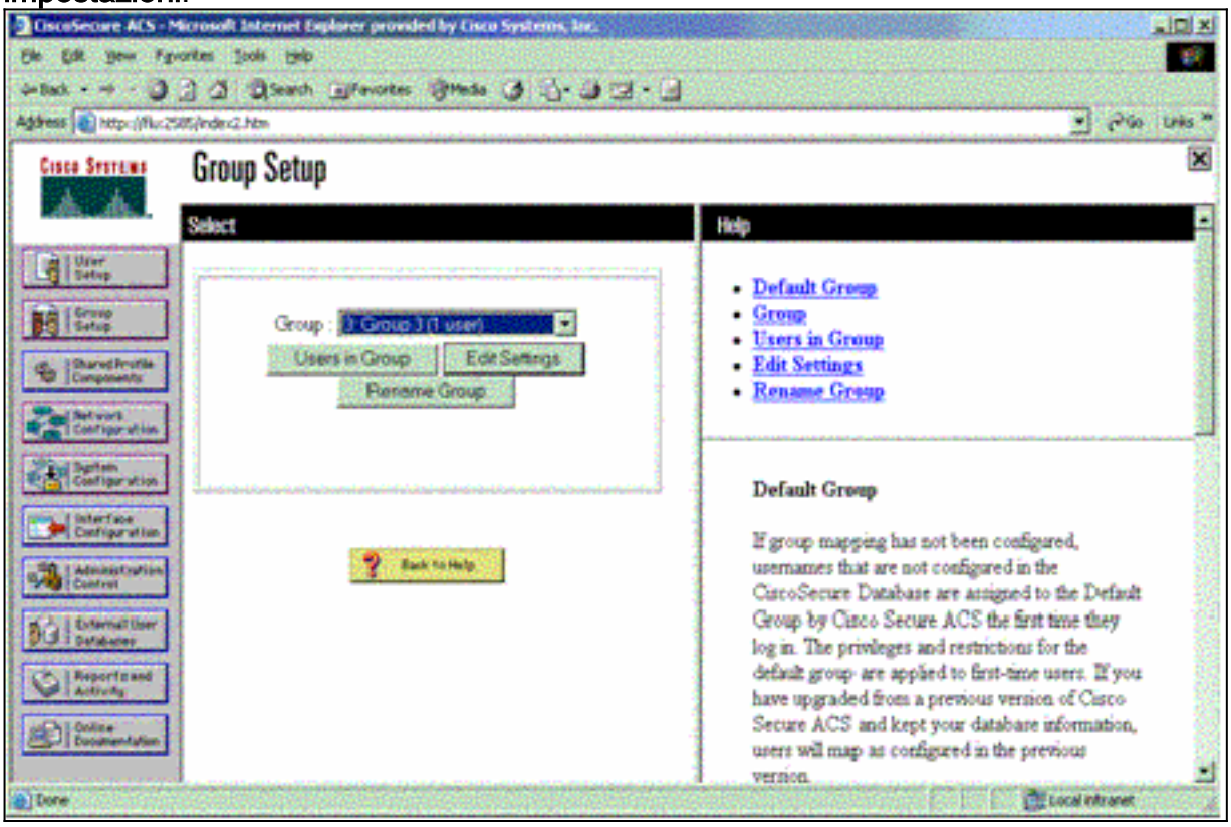


7. Scegliere il gruppo a cui è assegnato l'utente e selezionare **Utilizza impostazione gruppo**. Fare clic su
Invia.

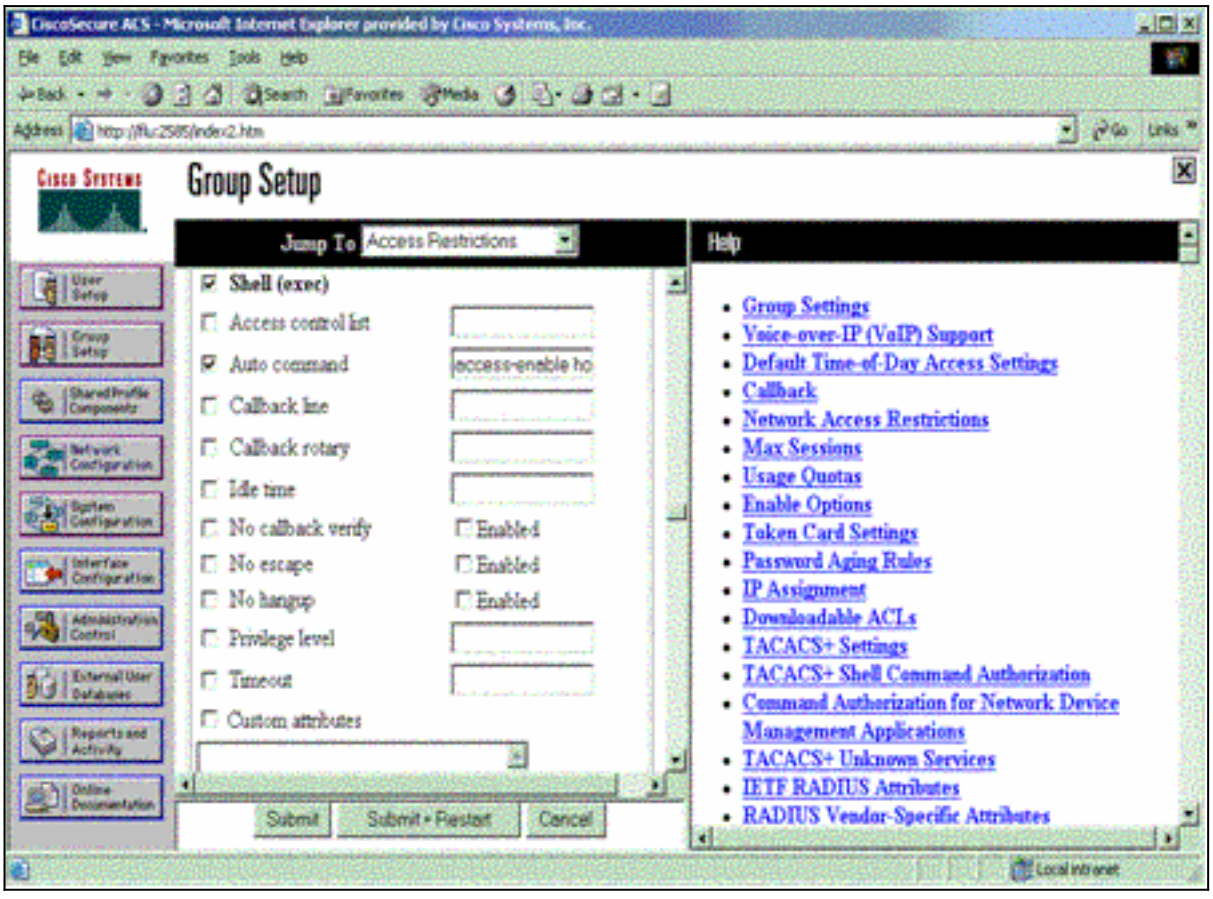


8. Fare clic su **Imposta gruppo**. Selezionare il gruppo al quale l'utente è stato assegnato nel passaggio 7. Fare clic su **Modifica**

impostazioni.



9. Scorrere fino alla sezione TACACS+ Settings. Selezionare la casella **Shell exec**. Selezionare la casella per il **comando Auto**. Immettere il comando automatico da eseguire dopo aver ottenuto l'autorizzazione dell'utente. In questo esempio viene utilizzato il comando **access-enable host timeout 10**. Fare clic su **Invia+Riavvia**.



[Risoluzione dei problemi di TACACS+]

Utilizzare questi comandi **debug** sul server NAS per risolvere i problemi relativi a TACACS+.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug tacacs authentication**: visualizza le informazioni sul processo di autenticazione TACACS+. Disponibile solo in alcune versioni del software. Se non disponibile, usare solo **debug tacacs**.
- **debug tacacs authorization**: visualizza le informazioni sul processo di autorizzazione TACACS+. Disponibile solo in alcune versioni del software. Se non disponibile, usare solo **debug tacacs**.
- **debug tacacs events**: visualizza le informazioni provenienti dal processo helper TACACS+. Disponibile solo in alcune versioni del software. Se non disponibile, usare solo **debug tacacs**.

Utilizzare questi comandi per risolvere i problemi relativi al server AAA:

- **debug aaa authentication**: visualizza le informazioni sull'autenticazione AAA/TACACS+.
- **debug aaa authorization**: visualizza le informazioni sull'autorizzazione AAA/TACACS+.

L'output di esempio del comando **debug** riportato di seguito mostra un processo di autenticazione e autorizzazione sul server ACS TACACS+ riuscito.

```
Router#show debug
General OS:
  TACACS+ events debugging is on
  TACACS+ authentication debugging is on
  TACACS+ authorization debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
======================================================
Router#
 AAA/BIND(00000009): Bind i/f
 AAA/AUTHEN/LOGIN (00000009): Pick method list 'default'
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication start request id 9
 TPLUS: Authentication start packet created for 9()
 TPLUS: Using server 10.48.66.53
 TPLUS(00000009)/0/NB_WAIT/82A2E088: Started 5 sec timeout
 TPLUS(00000009)/0/NB_WAIT: socket event 2
 TPLUS(00000009)/0/NB_WAIT: wrote entire 36 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: Would block while reading
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 16 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 28 bytes response
 TPLUS(00000009)/0/82A2E088: Processing the reply packet
 TPLUS: Received authen response status GET_USER (7)
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication continue request id 9
 TPLUS: Authentication continue packet generated for 9
 TPLUS(00000009)/0/WRITE/8347F3FC: Started 5 sec timeout
 TPLUS(00000009)/0/WRITE: wrote entire 22 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 16 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 28 bytes response
```

```
TPLUS(00000009)/0/8347F3FC: Processing the reply packet
TPLUS: Received authen response status GET_PASSWORD (8)
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9
TPLUS(00000009)/0/WRITE/8347EE4C: Started 5 sec timeout
TPLUS(00000009)/0/WRITE: wrote entire 25 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 6 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 18 bytes response
TPLUS(00000009)/0/8347EE4C: Processing the reply packet
TPLUS: Received authen response status PASS (2)
AAA/AUTHOR (0x9): Pick method list 'default'
TPLUS: Queuing AAA Authorization request 9 for processing
TPLUS: processing authorization request id 9
TPLUS: Protocol set to None .....Skipping
TPLUS: Sending AV service=shell
TPLUS: Sending AV cmd
TPLUS: Authorization request created for 9(tne-1)
TPLUS: using previously set server 10.48.66.53
  from group tacacs+
TPLUS(00000009)/0/NB_WAIT/8347F508: Started 5 sec timeout
TPLUS(00000009)/0/NB_WAIT: socket event 2
TPLUS(00000009)/0/NB_WAIT: wrote entire 60 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: Would block while reading
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 44 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 56 bytes response
TPLUS(00000009)/0/8347F508: Processing the reply packet
TPLUS: Processed AV autocmd=access-enable host timeout 10
TPLUS: received authorization response for 9: PASS
AAA/AUTHOR/EXEC(00000009): processing AV cmd=
AAA/AUTHOR/EXEC(00000009): processing AV
  autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000009): Authorization successful
```

Utilizzo di RADIUS

Configura RADIUS

Per utilizzare RADIUS, configurare un server RADIUS in modo che imponga l'autenticazione da eseguire sul server RADIUS con i parametri di autorizzazione (il comando automatico) da inviare nell'attributo 26 specifico del fornitore, come mostrato di seguito:

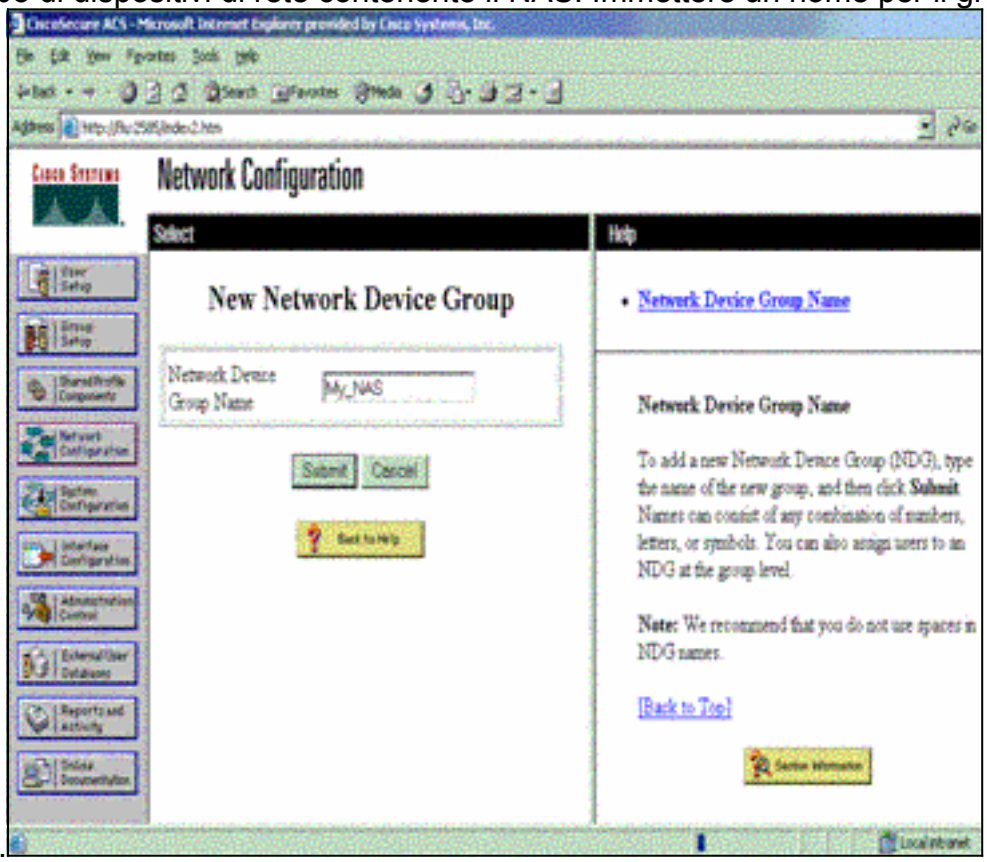
```
aaa new-model
!
!
aaa authentication login default group radius local
aaa authorization exec default group radius local
radius-server host 10.48.66.53 auth-port 1645
   acct-port 1646 key cisco123
```

Completare la procedura seguente per configurare RADIUS su Cisco Secure ACS per Windows:

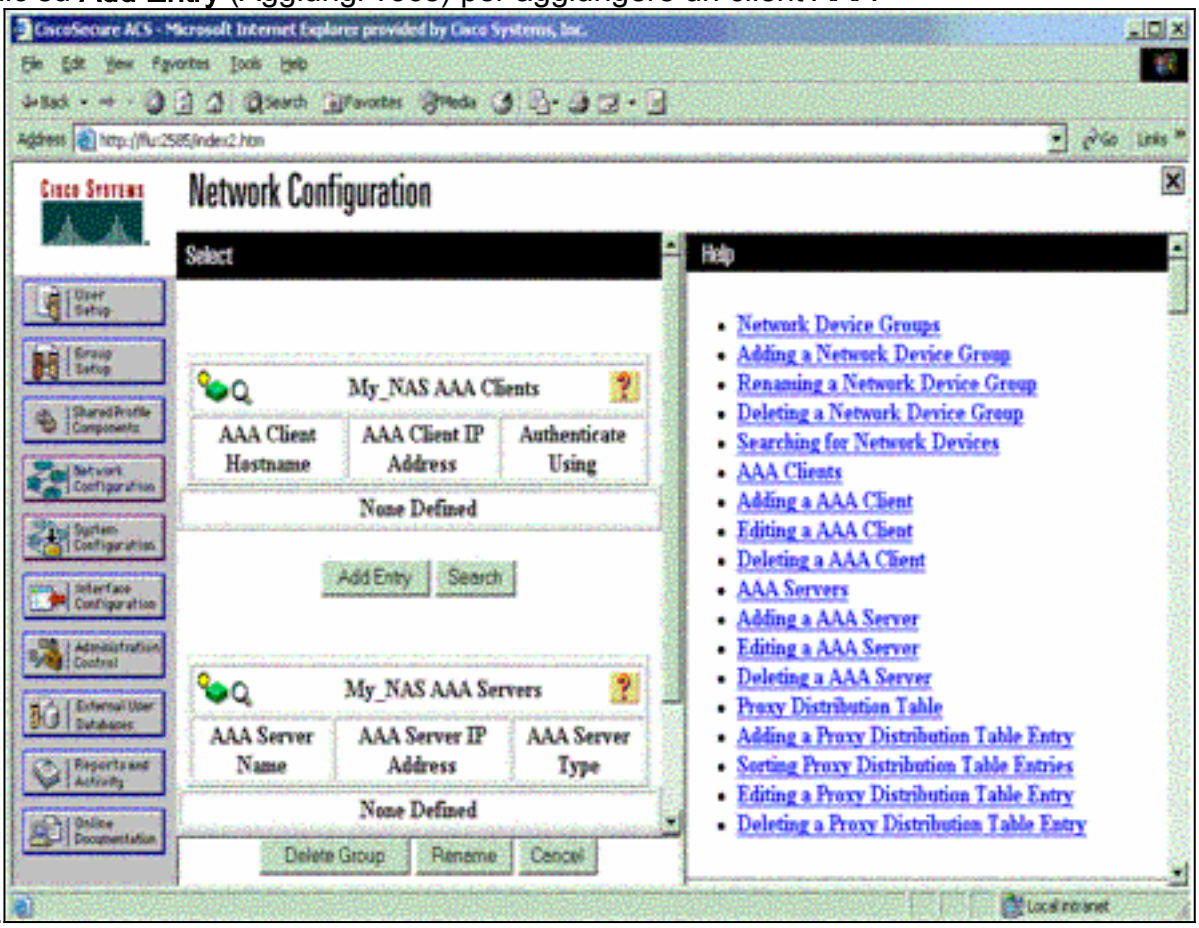
1. Aprire un browser Web e immettere l'indirizzo del server ACS nel formato **http://*<indirizzo_IP***

o nome_DNS>:2002. In questo esempio viene utilizzata una porta predefinita, ovvero 2002. Accedere come admin.

2. Fare clic su **Configurazione di rete**. Fare clic su **Add Entry** (Aggiungi voce) per creare un gruppo di dispositivi di rete contenente il NAS. Immettere un nome per il gruppo e fare clic su **Invia**.

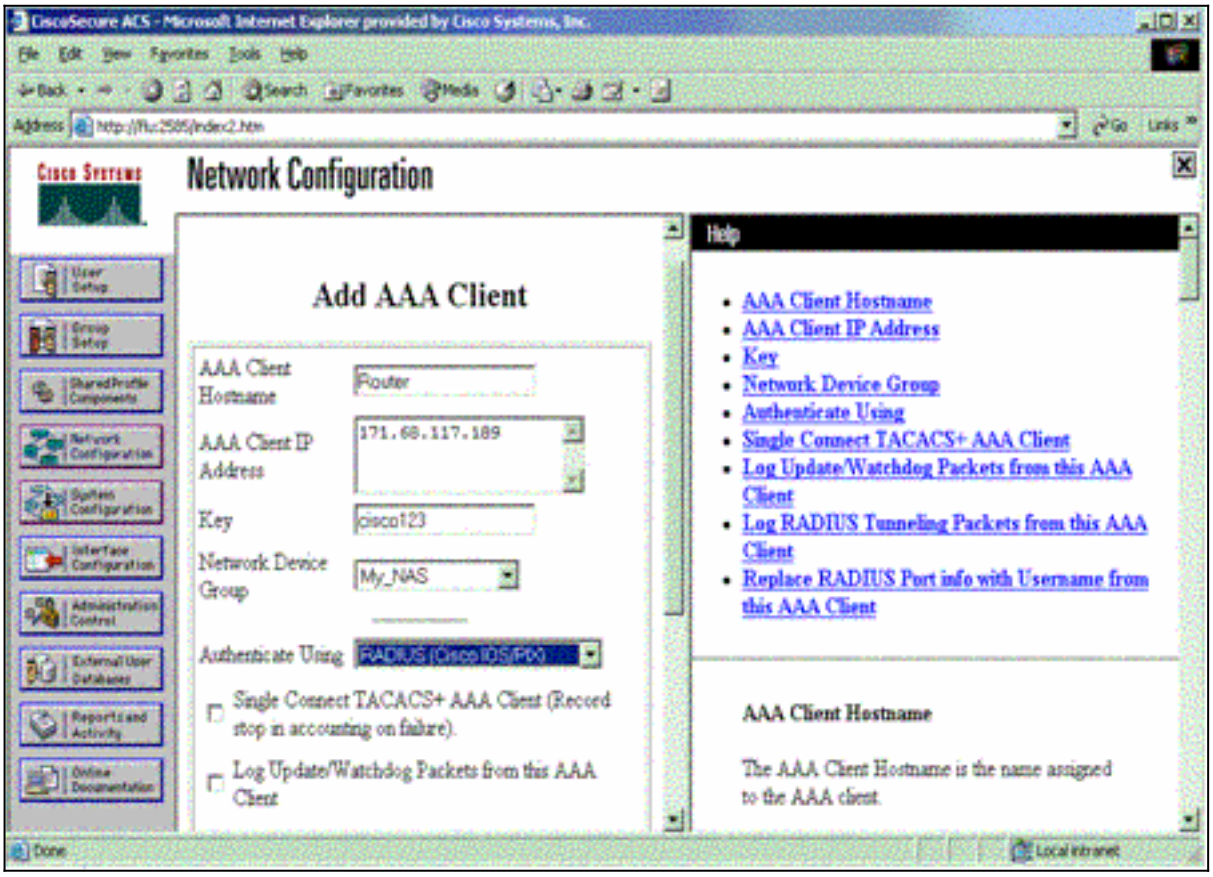


3. Fare clic su **Add Entry** (Aggiungi voce) per aggiungere un client AAA (NAS).

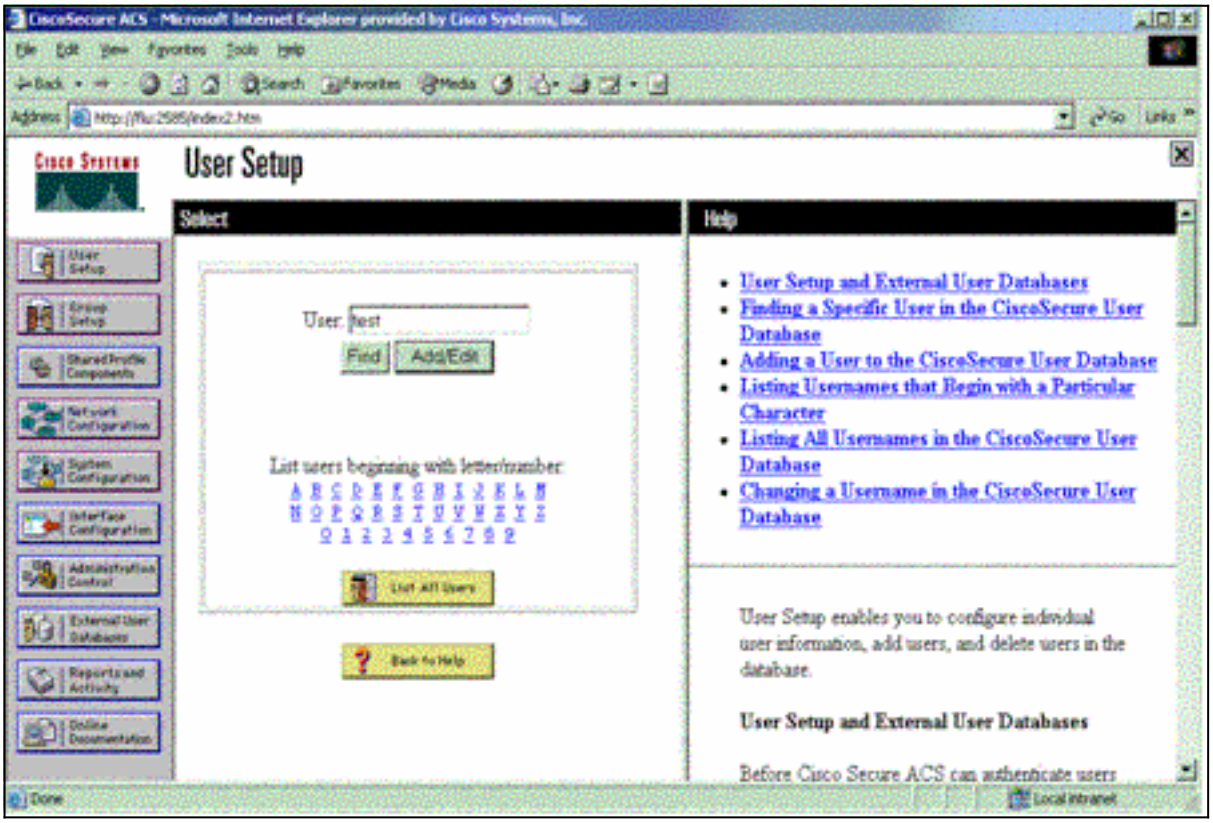


4. Immettere il nome host, l'indirizzo IP e la chiave utilizzata per crittografare la comunicazione

tra il server AAA e il server NAS. Selezionare **RADIUS (Cisco IOS/PIX)** come metodo di autenticazione. Al termine, fare clic su **Invia +Riavvia** per applicare le modifiche.

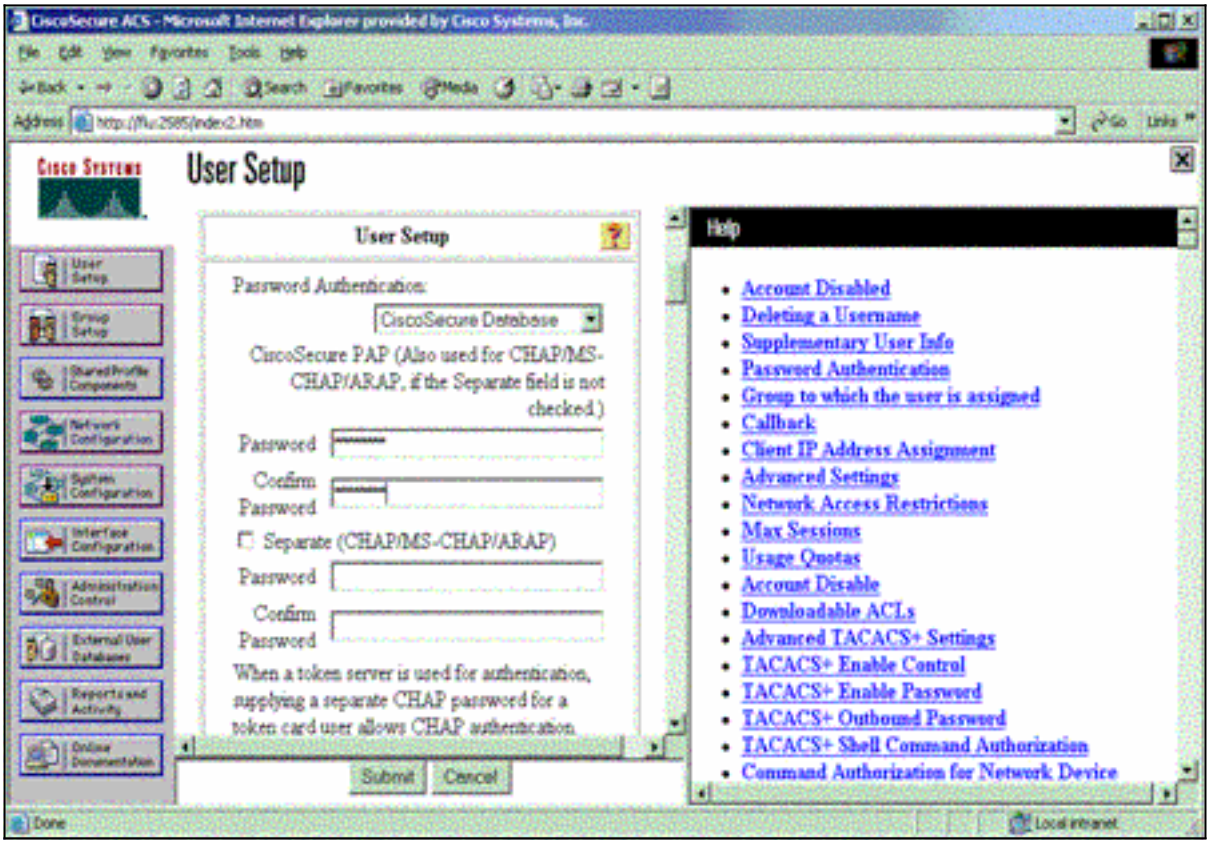


5. Fare clic su **User Setup**, immettere un ID utente e fare clic su **Add/Edit**.

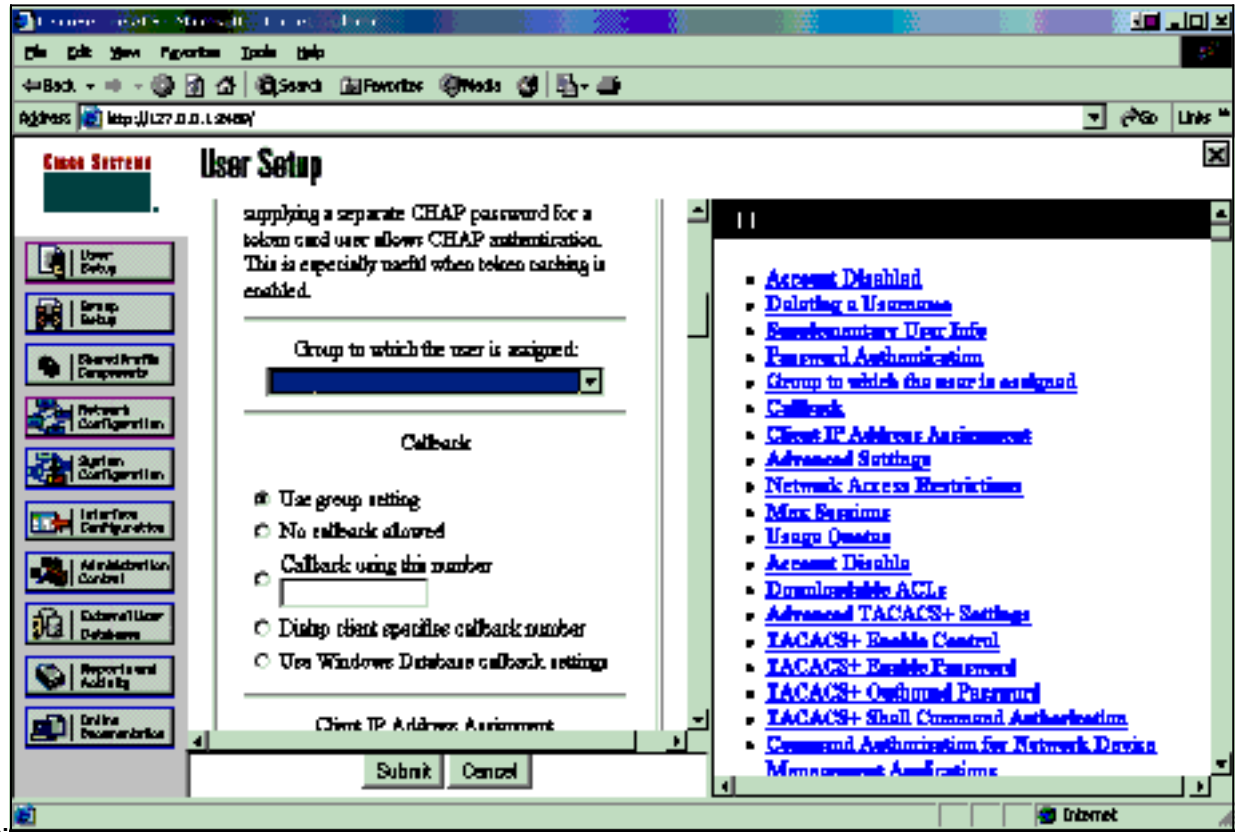


6. Scegliere un database per autenticare l'utente. In questo esempio, l'utente è "test" e per l'autenticazione viene utilizzato il database interno del server ACS. Immettere una password per l'utente e

confermarla.

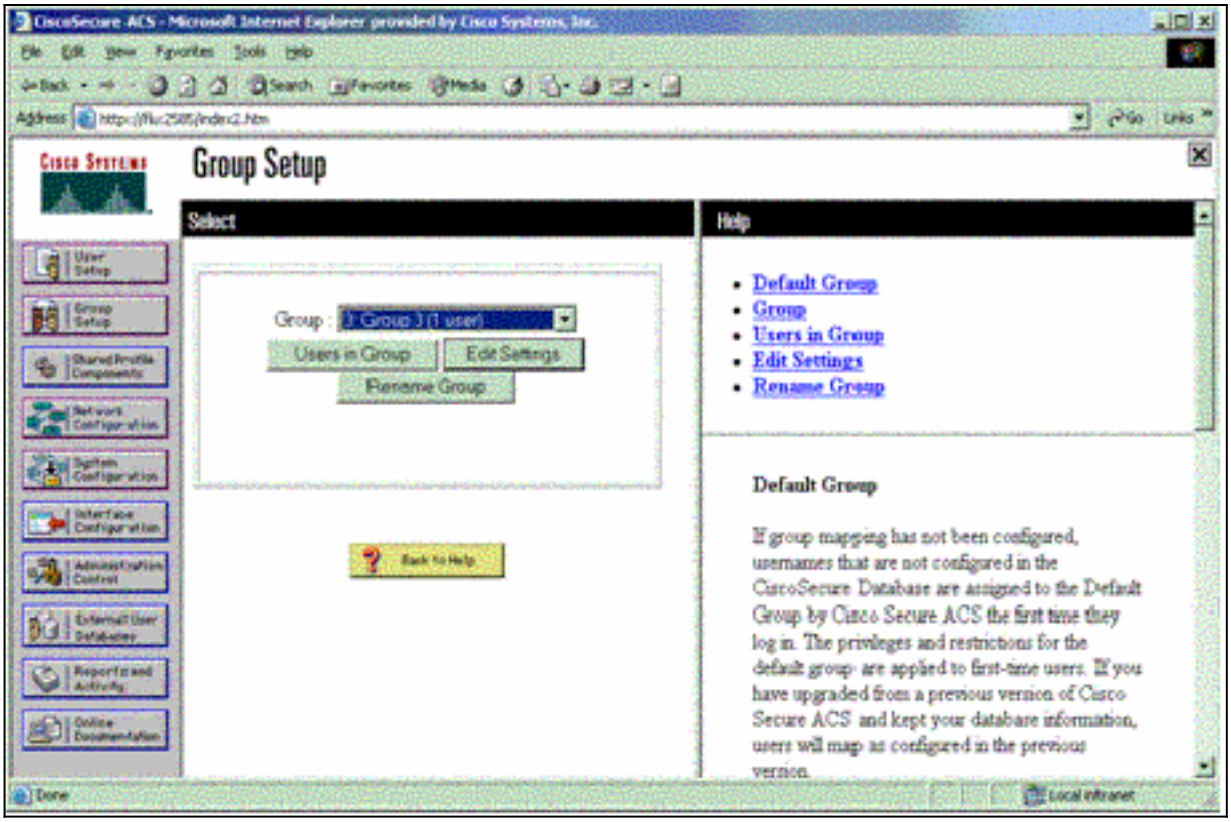


7. Scegliere il gruppo a cui è assegnato l'utente e selezionare **Utilizza impostazione gruppo**. Fare clic su

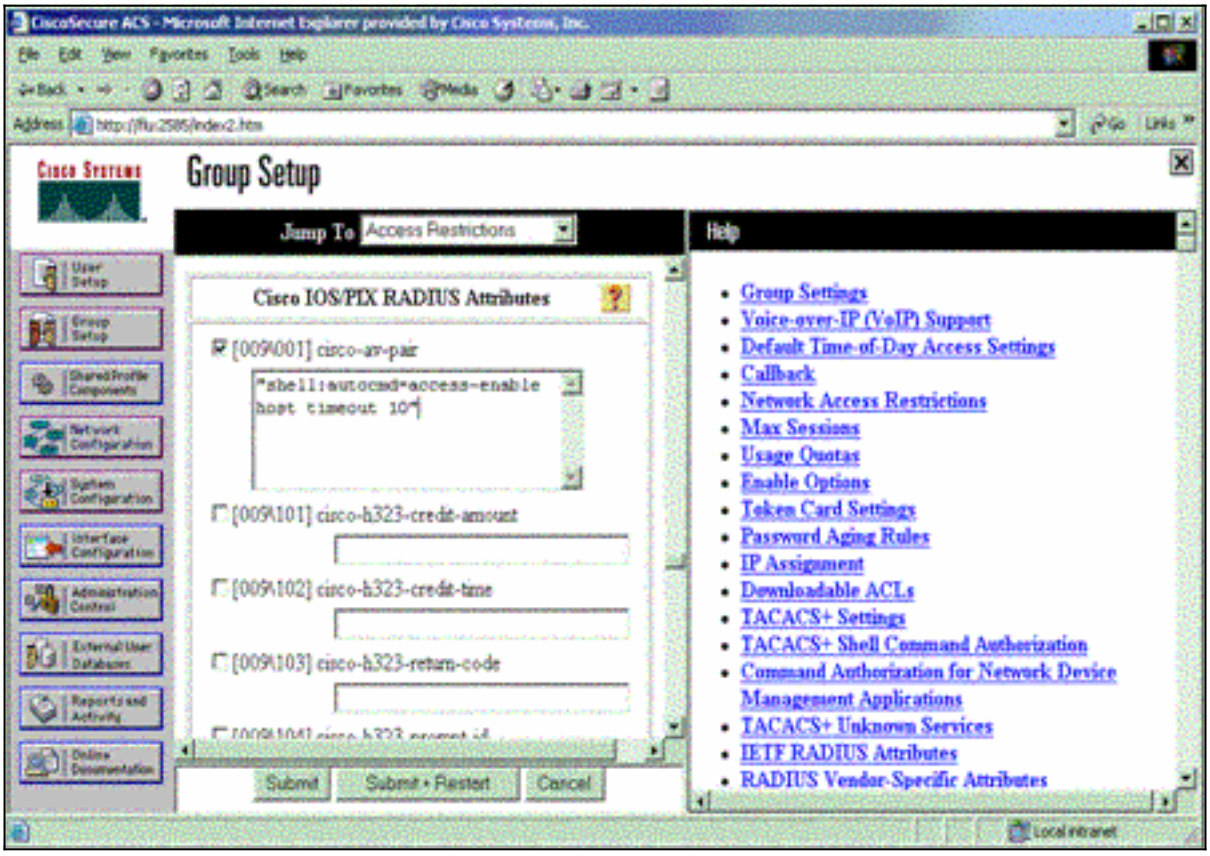


Invia.

8. Fare clic su **Imposta gruppo** e selezionare il gruppo al quale l'utente è stato assegnato nel passaggio precedente. Fare clic su **Modifica impostazioni**.



9. Scorrere fino alla sezione Attributi RADIUS Cisco IOS/PIX. Selezionare la casella per **cisco-av-pair**. Immettere il comando **shell** da eseguire dopo aver ottenuto l'autorizzazione dell'utente. In questo esempio viene utilizzata la **shell:autocmd=access-enable host timeout 10**. Fare clic su **Invia+Riavvia**.



Risoluzione dei problemi relativi a RADIUS

Utilizzare questi comandi di **debug** sul server NAS per risolvere i problemi relativi a RADIUS.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug radius** - Visualizza le informazioni associate a RADIUS.

Utilizzare questi comandi per risolvere i problemi relativi al server AAA:

- **debug aaa authentication**: visualizza le informazioni sull'autenticazione AAA/TACACS+.
- **debug aaa authorization**: visualizza le informazioni sull'autorizzazione AAA/TACACS+.

Nell'output di esempio del comando **debug** viene mostrato un processo di autenticazione e autorizzazione riuscito sull'ACS configurato per RADIUS.

```
Router#show debug
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on

Radius protocol debugging is on
Radius packet protocol debugging is on
=======================================================
Router#
 AAA/BIND(00000003): Bind i/f
 AAA/AUTHEN/LOGIN (00000003): Pick method list 'default'
 RADIUS/ENCODE(00000003): ask "Username: "
 RADIUS/ENCODE(00000003): send packet; GET_USER
 RADIUS/ENCODE(00000003): ask "Password: "
 RADIUS/ENCODE(00000003): send packet; GET_PASSWORD
 RADIUS:  AAA Unsupported     [152] 5
 RADIUS:   74 74 79                        [tty]
 RADIUS(00000003): Storing nasport 66 in rad_db
 RADIUS/ENCODE(00000003): dropping service type,
   "radius-server attribute 6 on-for-login-auth" is off
 RADIUS(00000003): Config NAS IP: 0.0.0.0
 RADIUS/ENCODE(00000003): acct_session_id: 1
 RADIUS(00000003): sending
 RADIUS/ENCODE: Best Local IP-Address 172.18.124.1
   for Radius-Server 10.48.66.53
 RADIUS(00000003): Send Access-Request to 10.48.66.53:1645
   id 21645/1, len 77
 RADIUS:  authenticator 5A 95 1F EA A7 94 99 E5 -
   BE B5 07 BD E9 05 5B 5D
 RADIUS:  User-Name           [1]   7   "test"
 RADIUS:  User-Password       [2]   18  *
 RADIUS:  NAS-Port            [5]   6   66
 RADIUS:  NAS-Port-Type       [61]  6   Virtual     [5]
 RADIUS:  Calling-Station-Id  [31]  14  "171.68.109.158"
 RADIUS:  NAS-IP-Address      [4]   6   171.68.117.189
 RADIUS: Received from id 21645/1 10.48.66.53:1645,
   Access-Accept, len 93
 RADIUS:  authenticator 7C 14 7D CB 33 19 97 19 -
   68 4B C3 FC 25 21 47 CD
 RADIUS:  Vendor, Cisco       [26]  51
 RADIUS:   Cisco AVpair       [1]   45
   "shell:autocmd=access-enable host timeout 10"
 RADIUS:  Class               [25]  22
 RADIUS:   43 49 53 43 4F 41 43 53 3A 61 63 31 32 37 63 30
   [CISCOACS:ac127c0]
 RADIUS:   31 2F 36 36                  [1/66]
 RADIUS(00000003): Received from id 21645/1
 AAA/AUTHOR/EXEC(00000003): processing AV
```

```
   autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000003): Authorization successful
```

Informazioni correlate

- Cisco IOS Lock-and-Key Security
- Pagina di supporto TACACS/TACACS+
- Documentazione relativa a TACACS+ in IOS
- Pagina di supporto RADIUS
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems