ASA 8.3: Autenticazione TACACS con ACS 5.X

Sommario

Introduzione

In questo documento viene illustrato come configurare l'appliance di sicurezza per l'autenticazione degli utenti per l'accesso alla rete.

Prerequisiti

Requisiti

In questo documento si presume che le appliance ASA (Adaptive Security Appliance) siano completamente operative e configurate per consentire a Cisco Adaptive Security Device Manager (ASDM) o alla CLI di apportare modifiche alla configurazione.

Nota: per ulteriori informazioni su come consentire la configurazione remota del dispositivo da parte di ASDM, fare riferimento a Consenti accesso HTTPS per ASDM.

Componenti usati

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

- Software Cisco Adaptive Security Appliance versione 8.3 e successive
- Cisco Adaptive Security Device Manager versione 6.3 e successive

- Cisco Secure Access Control Server 5.x

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.

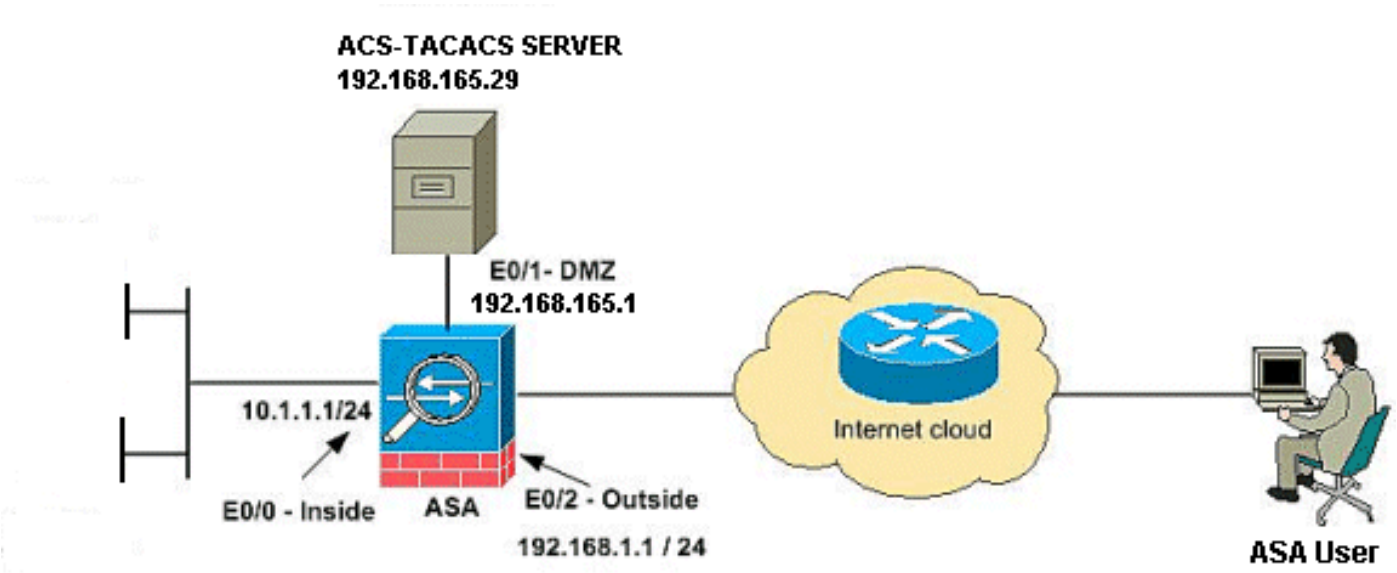
Configurazione

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

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Configurazione dell'ASA per l'autenticazione dal server ACS tramite CLI

Per autenticare l'appliance ASA dal server ACS, attenersi alla seguente configurazione:

```
!--- configuring the ASA for TACACS server ASA(config)# aaa-server cisco protocol tacacs+
ASA(config-aaa-server-group)# exit !--- Define the host and the interface the ACS server is on.
```

```
ASA(config)# aaa-server cisco (DMZ) host 192.168.165.29 ASA(config-aaa-server-host)# key cisco
!--- Configuring the ASA for HTTP and SSH access using ACS and fallback method as LOCAL
authentication. ASA(config)#aaa authentication ssh console cisco LOCAL ASA(config)#aaa
authentication http console cisco LOCAL
```

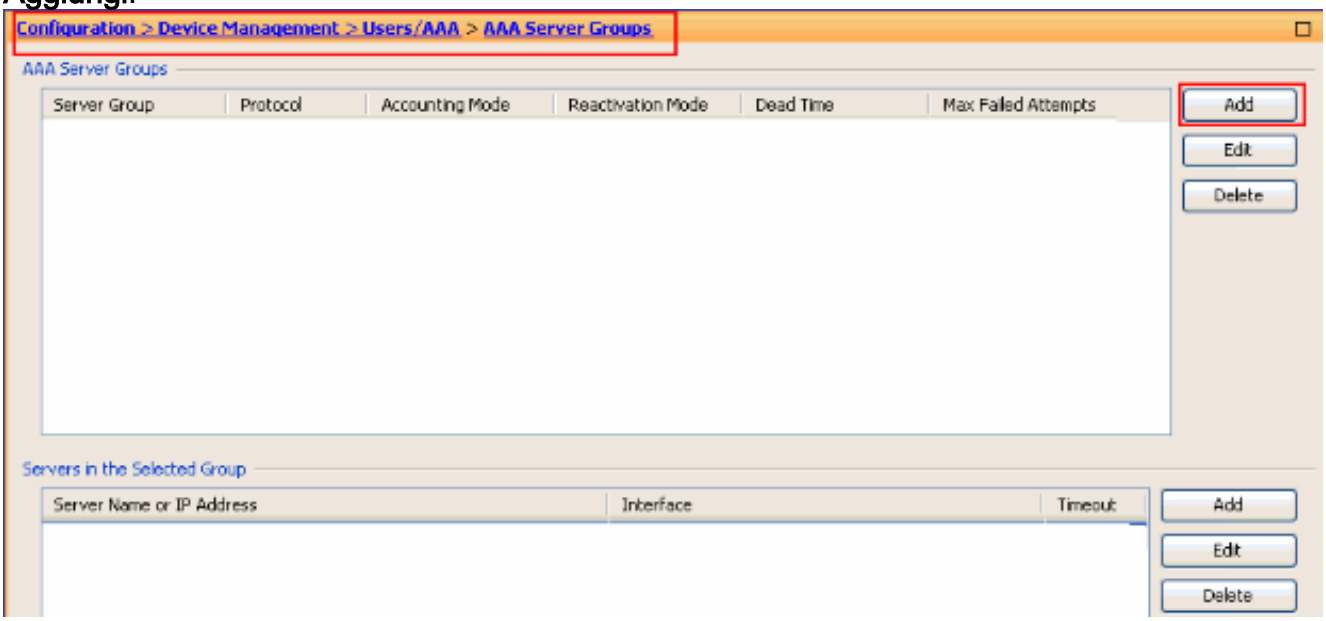
Nota: creare un utente locale sull'appliance ASA usando il comando **cisco password cisco privilege 15** per accedere all'appliance ASDM con autenticazione locale quando l'appliance ACS non è disponibile.

Configurazione di ASA per l'autenticazione dal server ACS con ASDM

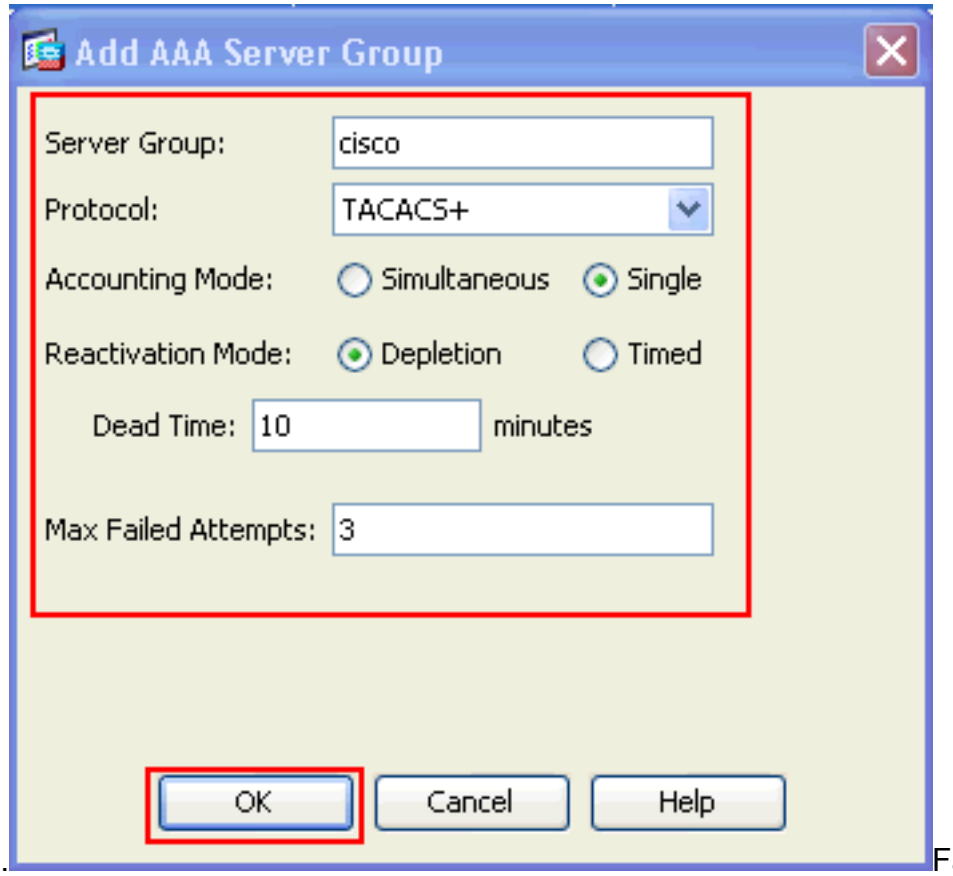
Procedura ASDM

Per configurare l'ASA per l'autenticazione dal server ACS, completare la procedura seguente:

1. Per creare un gruppo di server AAA, scegliere **Configurazione > Gestione dispositivi > Utenti/AAA > Gruppi** di **server** AAA **> Aggiungi**.

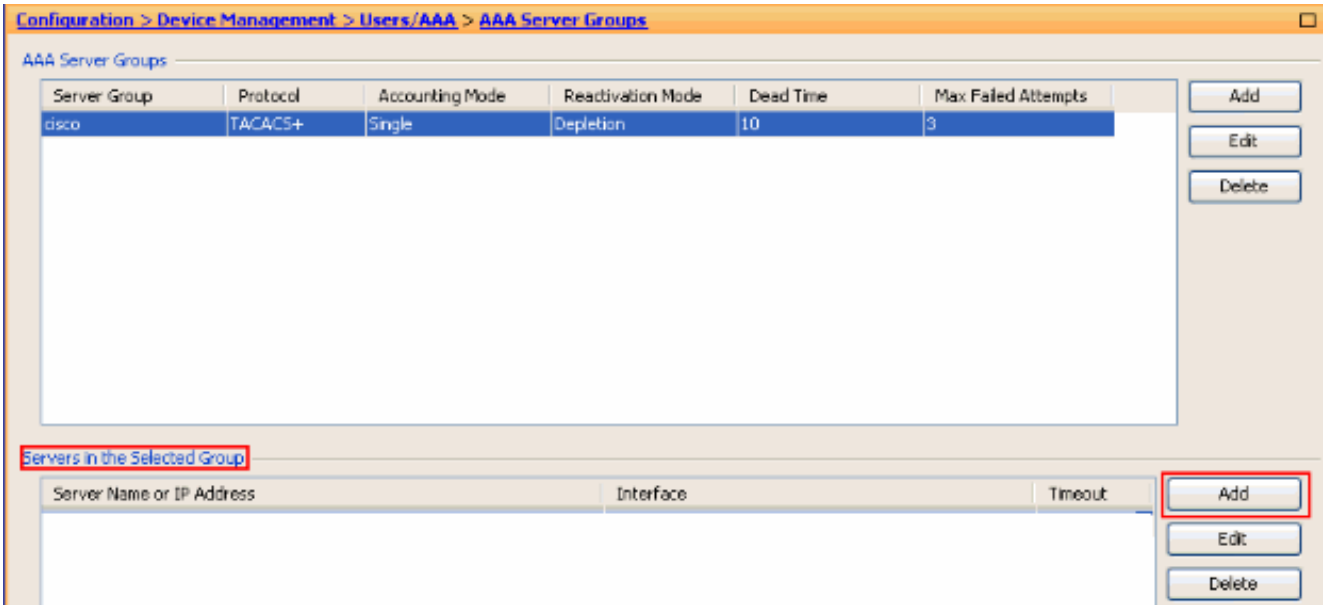


2. Specificare i dettagli del **gruppo di server AAA** nella finestra **Aggiungi gruppo di server AAA**, come mostrato. Il protocollo utilizzato è **TACACS+** e il gruppo di server creato è

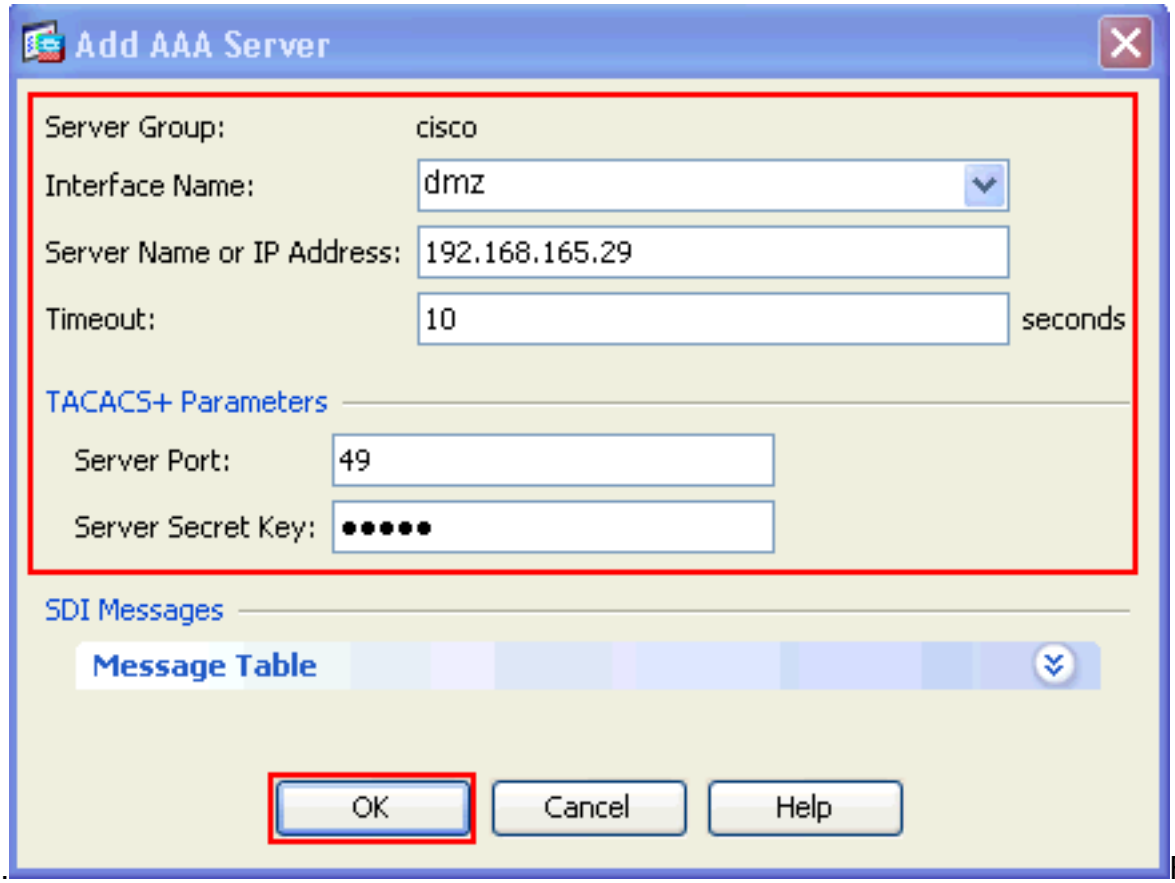


cisco. Fare clic su **OK**.

3. Per aggiungere il server AAA, selezionare **Configurazione > Gestione dispositivi > Utenti/AAA >** Gruppi di server AAA, quindi fare clic su **Aggiungi** in **Server nel gruppo selezionato**.

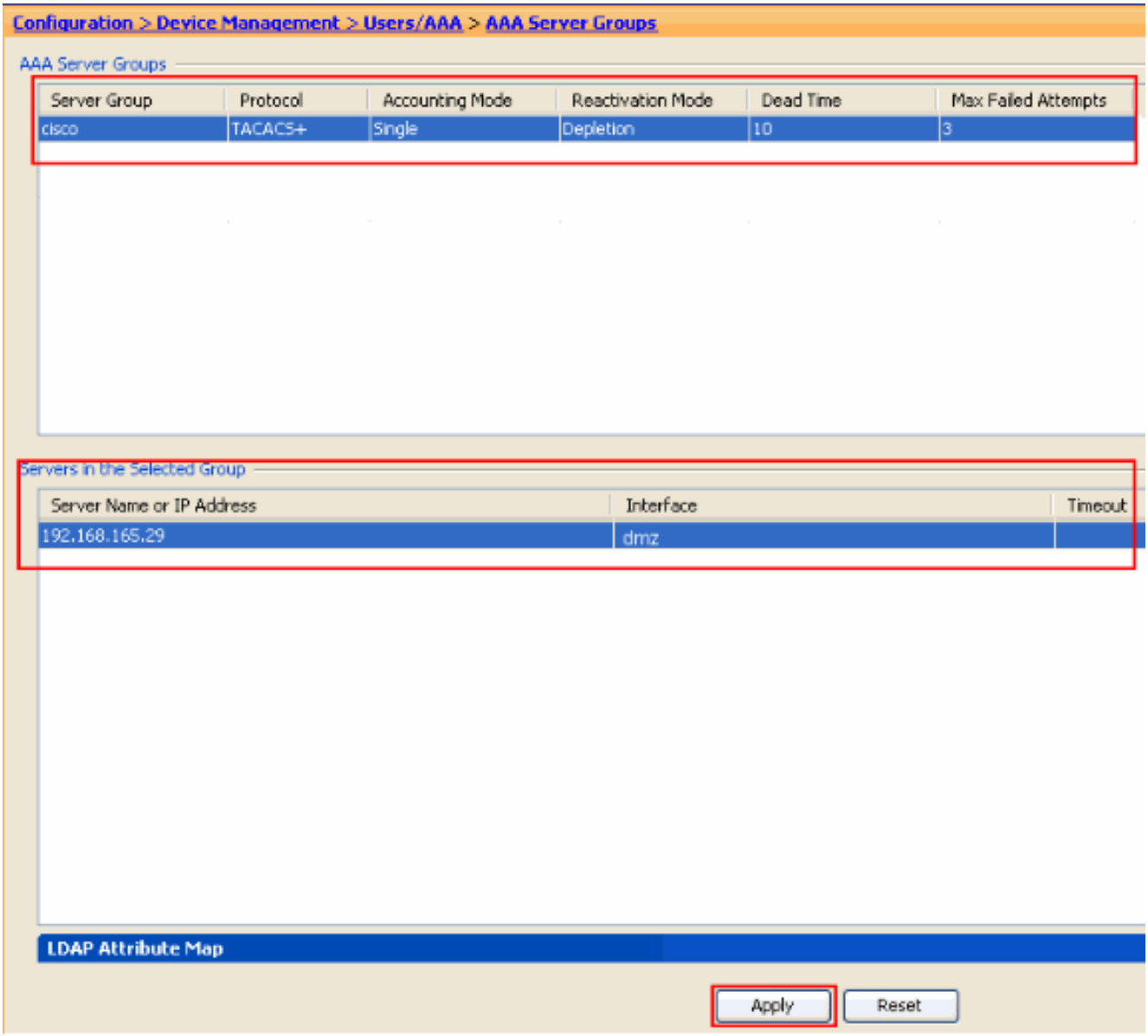


4. Specificare i dettagli del **server AAA** nella finestra **Add AAA Server** (Aggiungi server AAA), come mostrato. Il gruppo di server utilizzato è

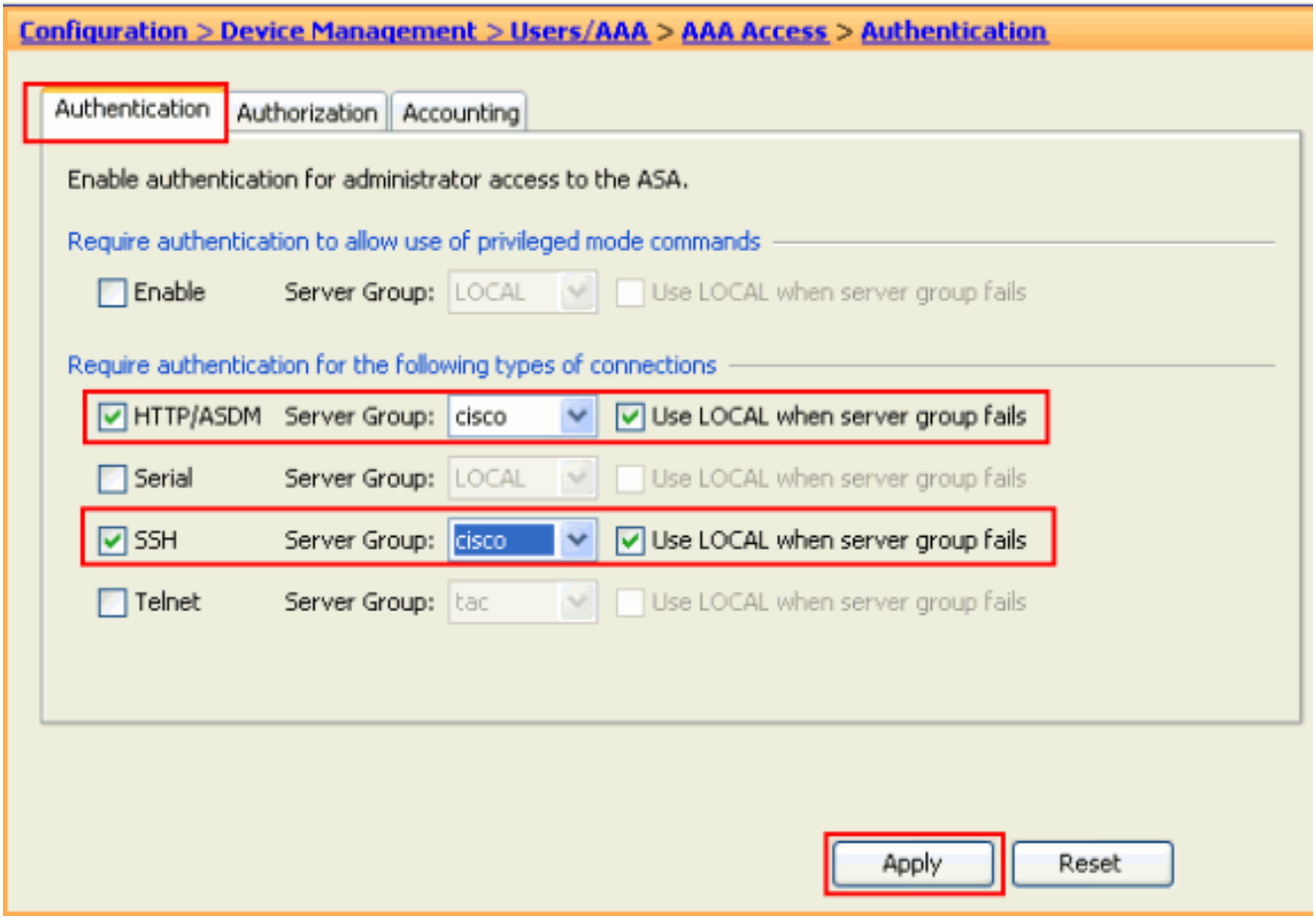


cisco.Fare clic su **OK**, quindi su **Applica**.Il **gruppo di server AAA** e il **server AAA** sono configurati sull'appliance ASA.

5. Fare clic su **Apply**
   (Applica).



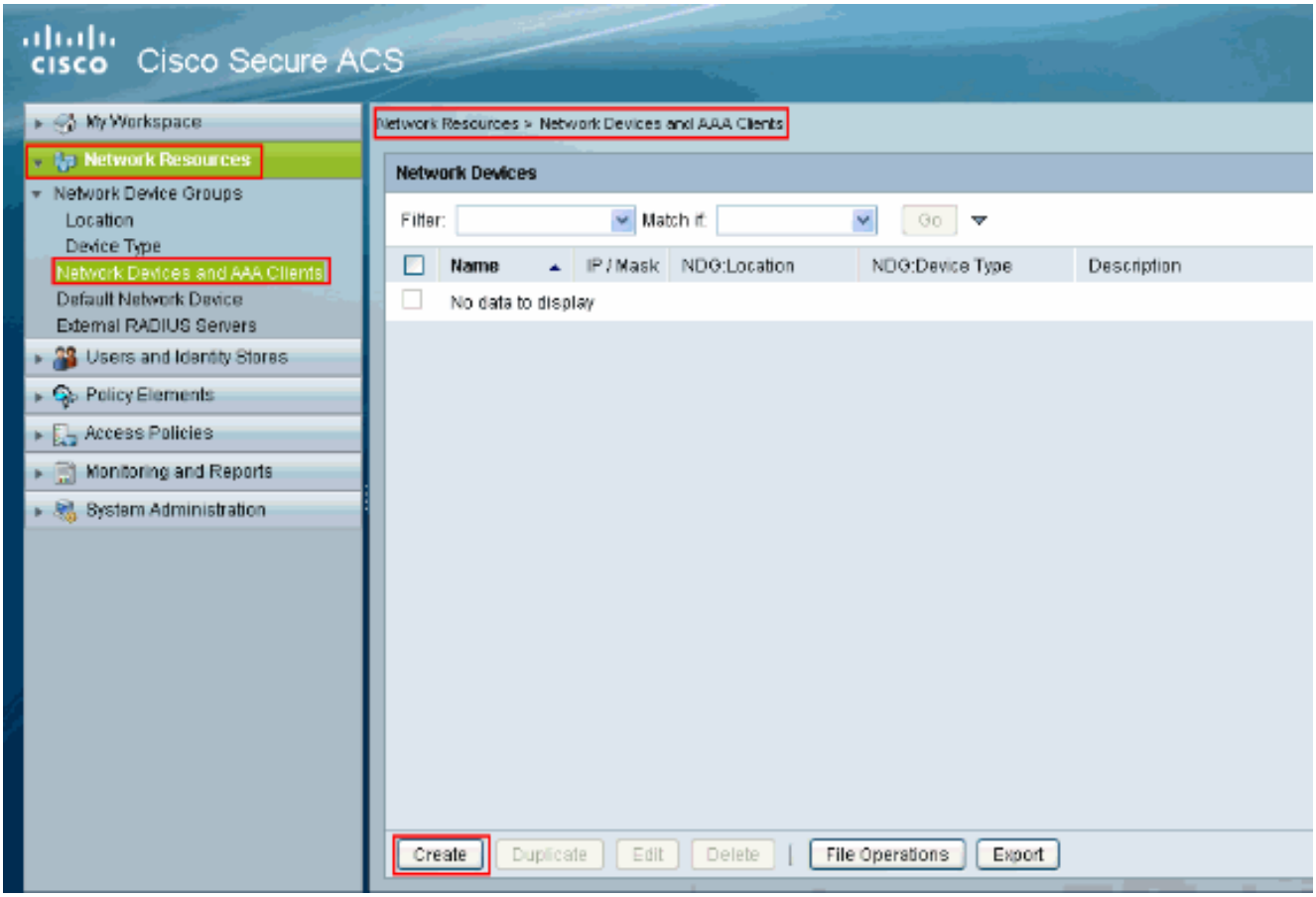
6. Scegliere **Configurazione > Gestione dispositivi > Utenti/AAA > Accesso AAA > Autenticazione** e fare clic sulle caselle di controllo accanto a **HTTP/ASDM** e **SSH**. Quindi, selezionare **cisco** come gruppo di server e fare clic su **Apply** (Applica).



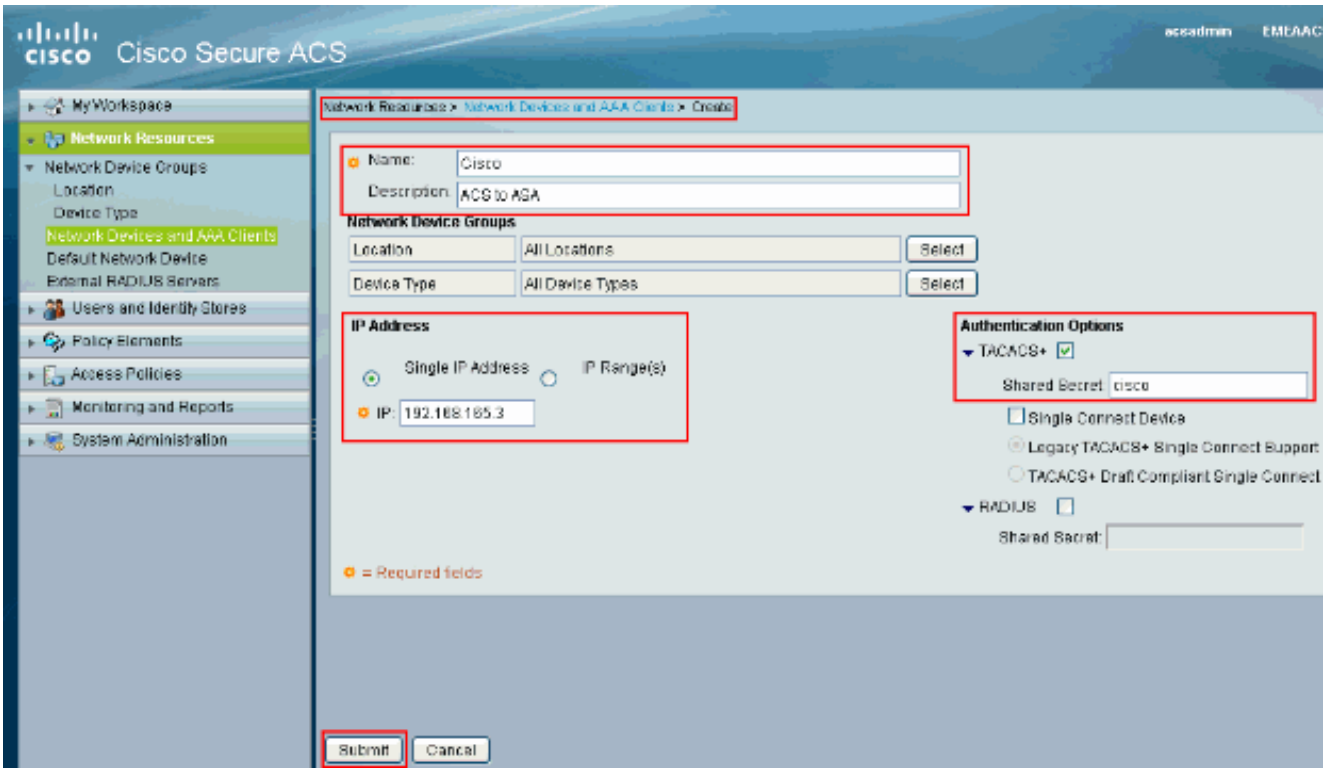
Configurazione di ACS come server TACACS

Completare questa procedura per configurare l'ACS come server TACACS:

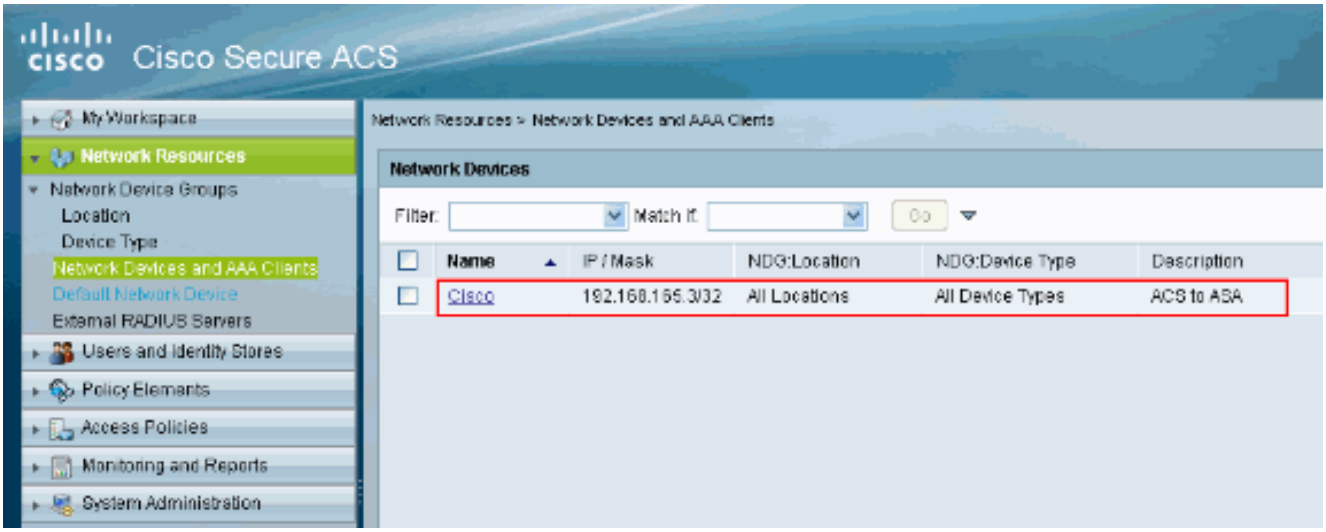
1. Per aggiungere l'appliance ASA al server ACS, selezionare **Risorse di rete > Dispositivi di rete e client AAA**, quindi fare clic su **Crea**.



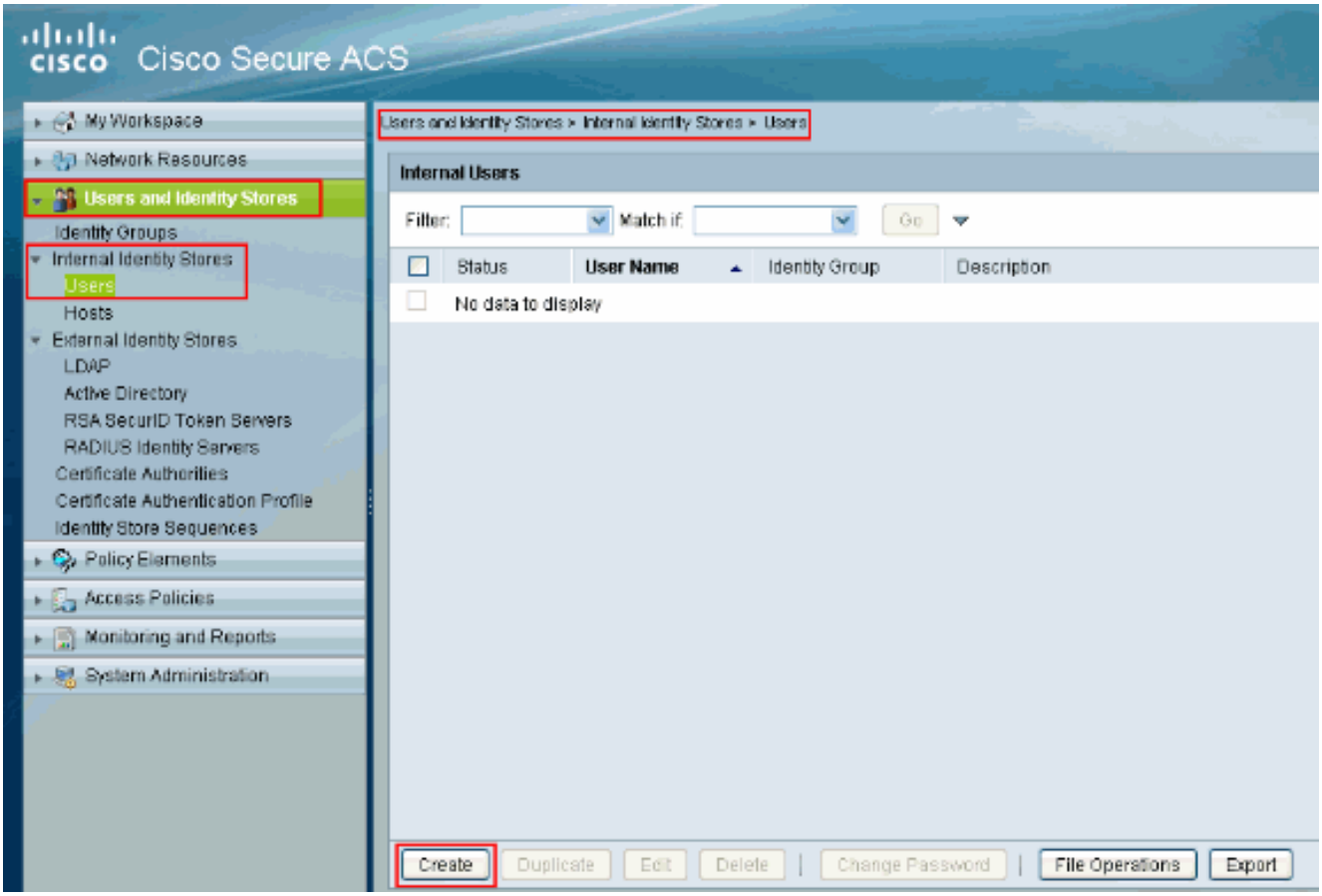
2. Fornire le informazioni richieste sul **client** (qui ASA è il client) e fare clic su **Submit**. In questo modo, l'appliance ASA può essere aggiunta al server ACS. I dettagli includono l'**indirizzo IP** dell'ASA e i dettagli **del server TACACS**.



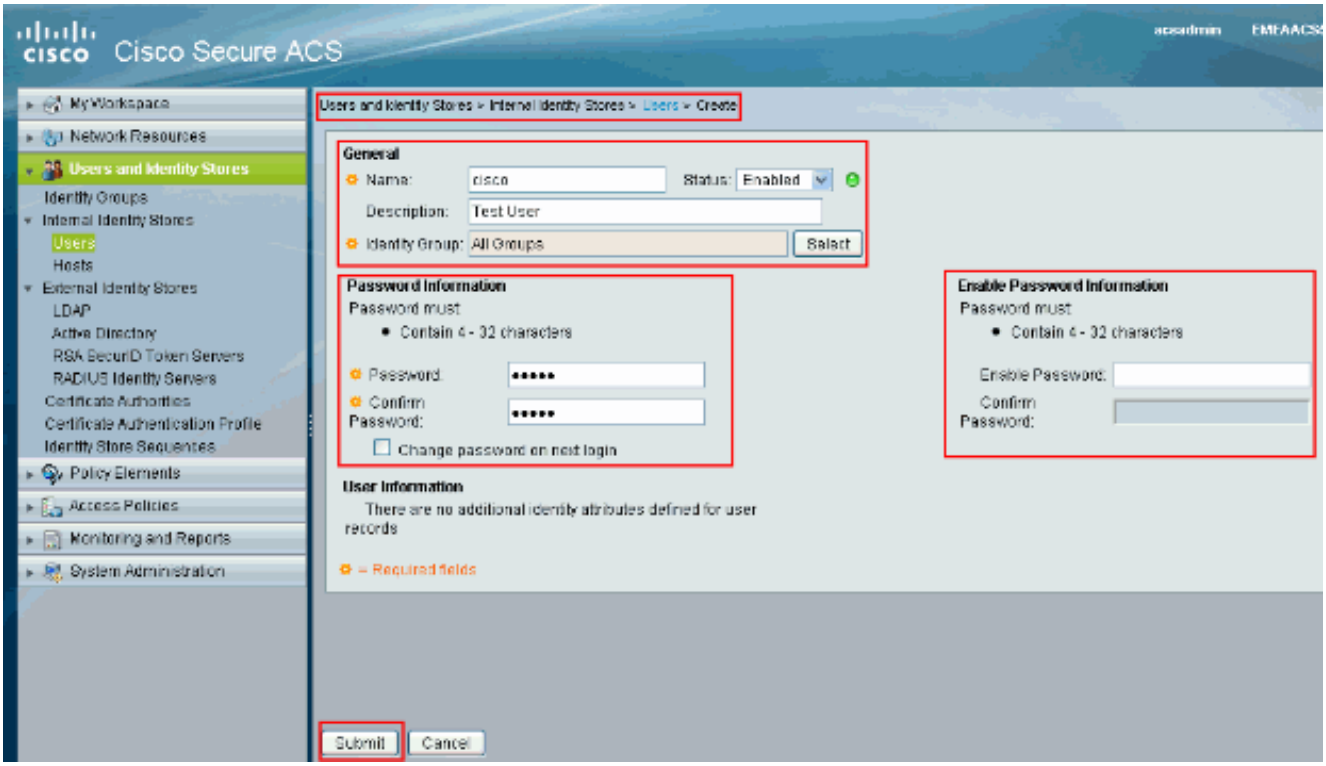
Il client **Cisco** verrà aggiunto al server ACS.



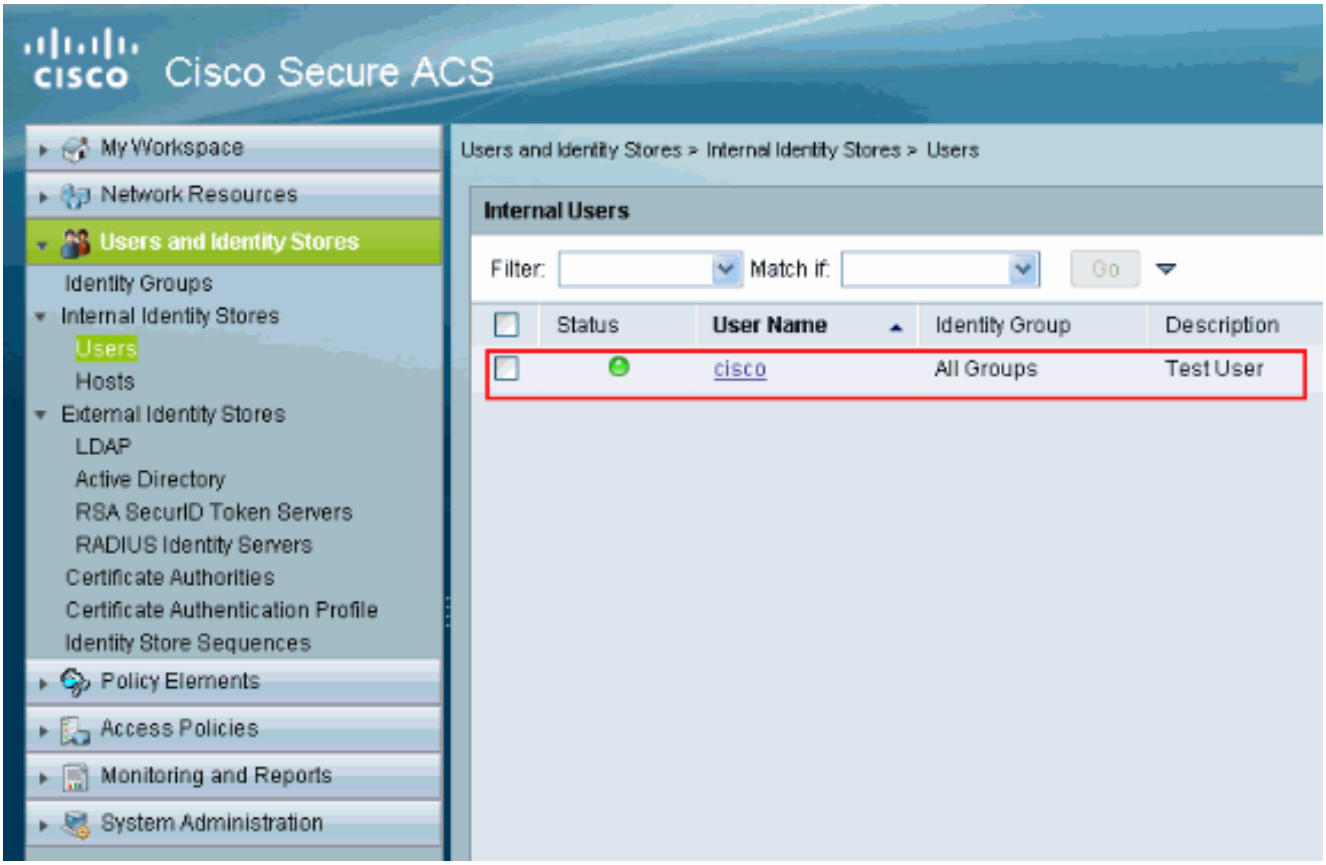
3. Scegliere **Utenti e archivi identità > Archivi identità interni > Utenti** e fare clic su **Crea** per creare un nuovo
utente.



4. Fornire le informazioni su **Nome, Password e Abilita password**. **L'abilitazione della password è facoltativa**. Al termine, fare clic su
Invia.



L'utente **cisco** verrà aggiunto al server ACS.

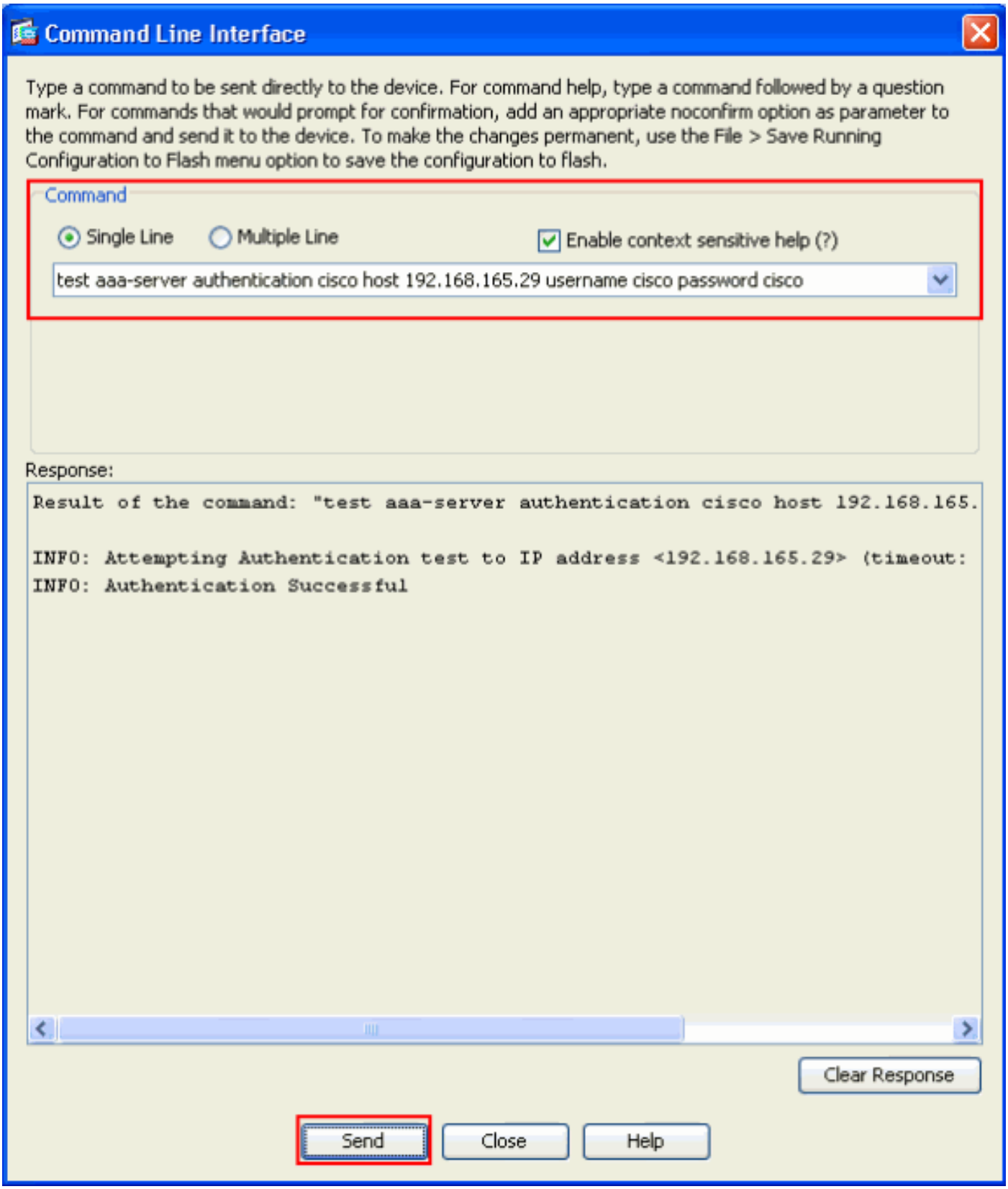


Verifica

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

Per verificare il corretto funzionamento della configurazione, **usare il** comando **cisco password cisco 192.168.165.29 username cisco host 192.168.165.29** username. Nell'immagine viene mostrata la riuscita dell'autenticazione e l'utente che si connette all'appliance ASA viene

autenticato dal server ACS.



Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Risoluzione dei problemi

Errore: AAA Contrassegno di TACACS+ server x.x.x.x in gruppo di server aaa come

NON RIUSCITO

Questo messaggio indica che Cisco ASA ha perso la connettività con il server x.x.x.x. Verificare di disporre di una connettività valida su tcp 49 al server x.x.x.x dall'appliance ASA. Inoltre, è possibile aumentare il timeout sull'appliance ASA per il server TACACS+ da 5 al numero di secondi desiderato in caso di latenza della rete. L'appliance ASA non invierà una richiesta di autenticazione al server x.x.x.x con errori. Tuttavia, utilizzerà il server successivo nel gruppo di tacacs aaa-server.

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance - Pagina di supporto
- Riferimenti per i comandi di Cisco ASA serie 5500 Adaptive Security Appliance
- Cisco Adaptive Security Device Manager
- Pagina di supporto per la negoziazione IPsec/i protocolli IKE
- Cisco Secure Access Control Server per Windows
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems