ASA 8.3:使用ACS 5.X的TACACS身份驗證

目錄

簡介

本文檔提供有關如何配置安全裝置以對使用者進行網路訪問驗證的資訊。

必要條件

需求

本文檔假設自適應安全裝置(ASA)完全可運行且配置為允許思科自適應安全裝置管理器(ASDM)或CLI進行配置更改。

註：有關如何允許ASDM遠端配置裝置的詳細資訊，請參閱允許ASDM進行HTTPS訪問。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科自適應安全裝置軟體版本8.3及更高版本
- 思科自適應安全裝置管理器6.3版及更高版本
- 思科安全存取控制伺服器5.x

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

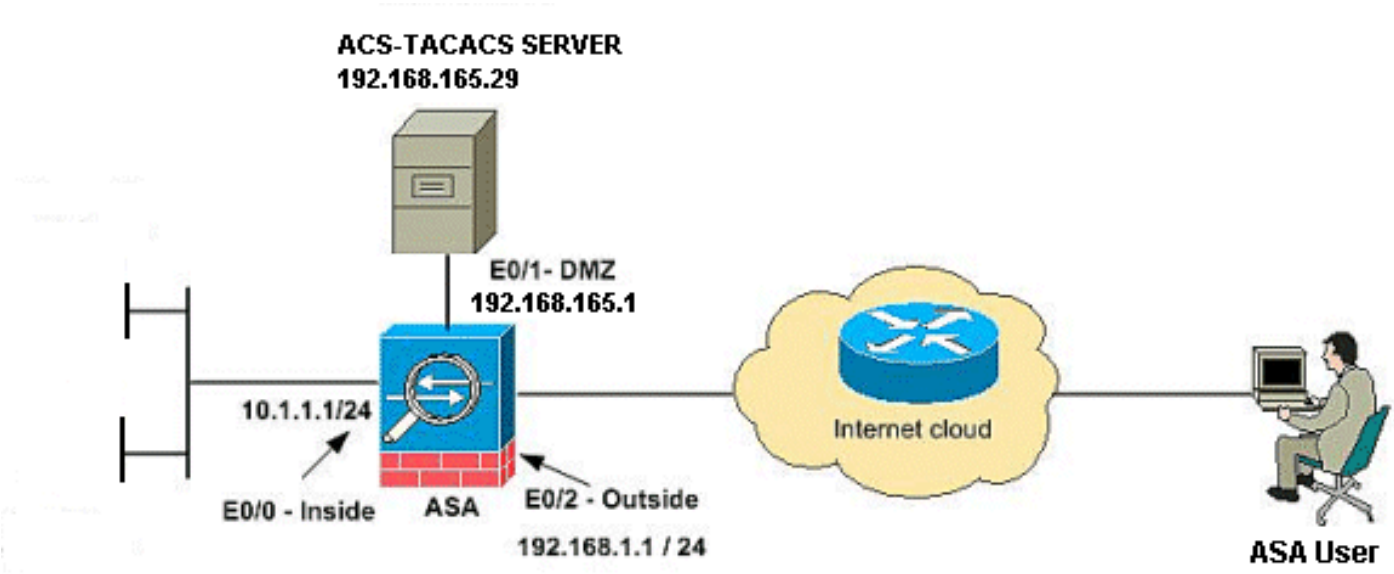
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用 Command Lookup Tool(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



注意：此配置中使用的IP編址方案在Internet上不能合法路由。它們是在實驗室環境中使用的RFC 1918地址。

使用CLI配置ASA以從ACS伺服器進行身份驗證

為ASA執行以下配置以從ACS伺服器進行身份驗證：

```
!--- 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
```

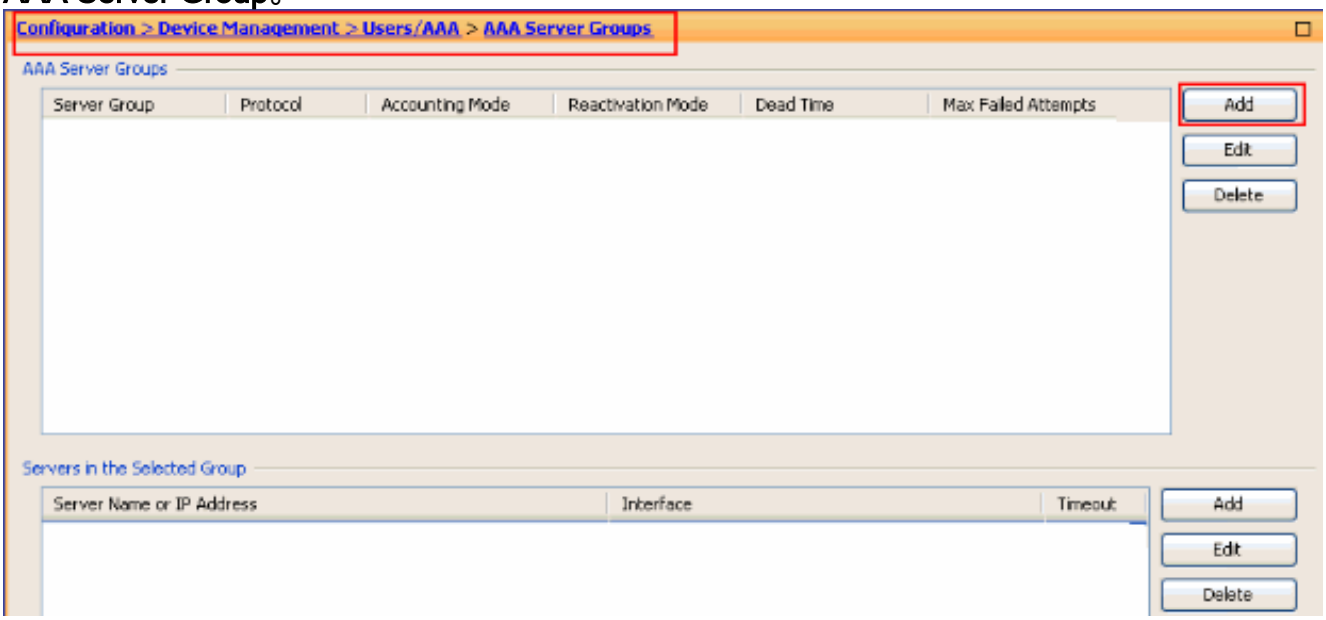
注意：在ASA上使用username cisco password cisco privilege 15 命令建立本地使用者，以便在ACS不可用時通過本地身份驗證訪問ASDM。

使用ASDM配置ASA以從ACS伺服器進行身份驗證

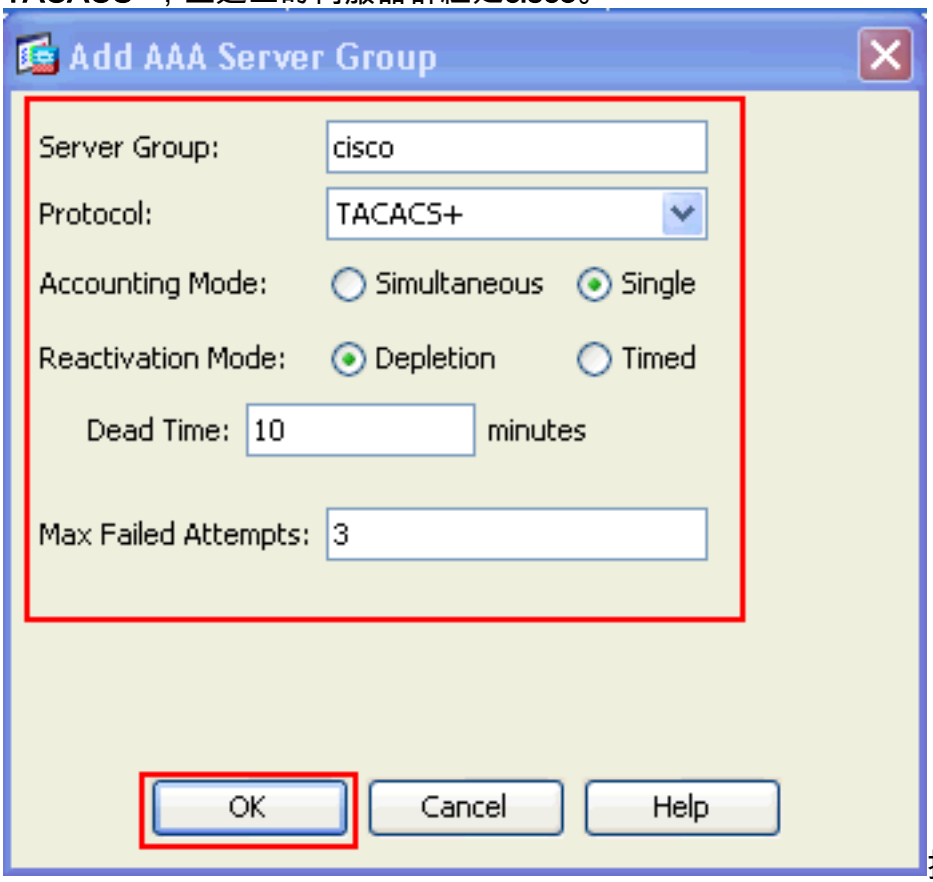
ASDM過程

完成以下步驟，以便從ACS伺服器配置ASA進行身份驗證：

1. 選擇**Configuration > Device Management > Users/AAA > AAA Server Groups > Add**以建立**AAA Server Group**。

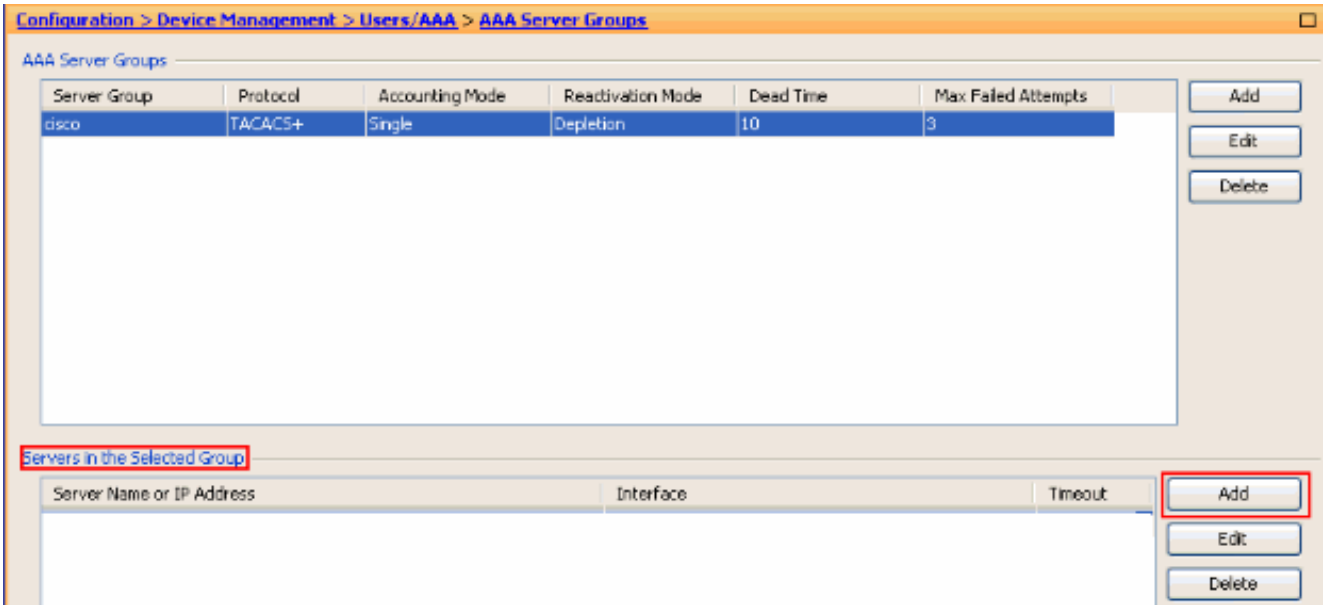


2. 在**Add AAA Server Group**視窗中提供**AAA Server Group**詳細資訊，如下所示。使用的協定是**TACACS+**，且建立的伺服器群組是**cisco**。

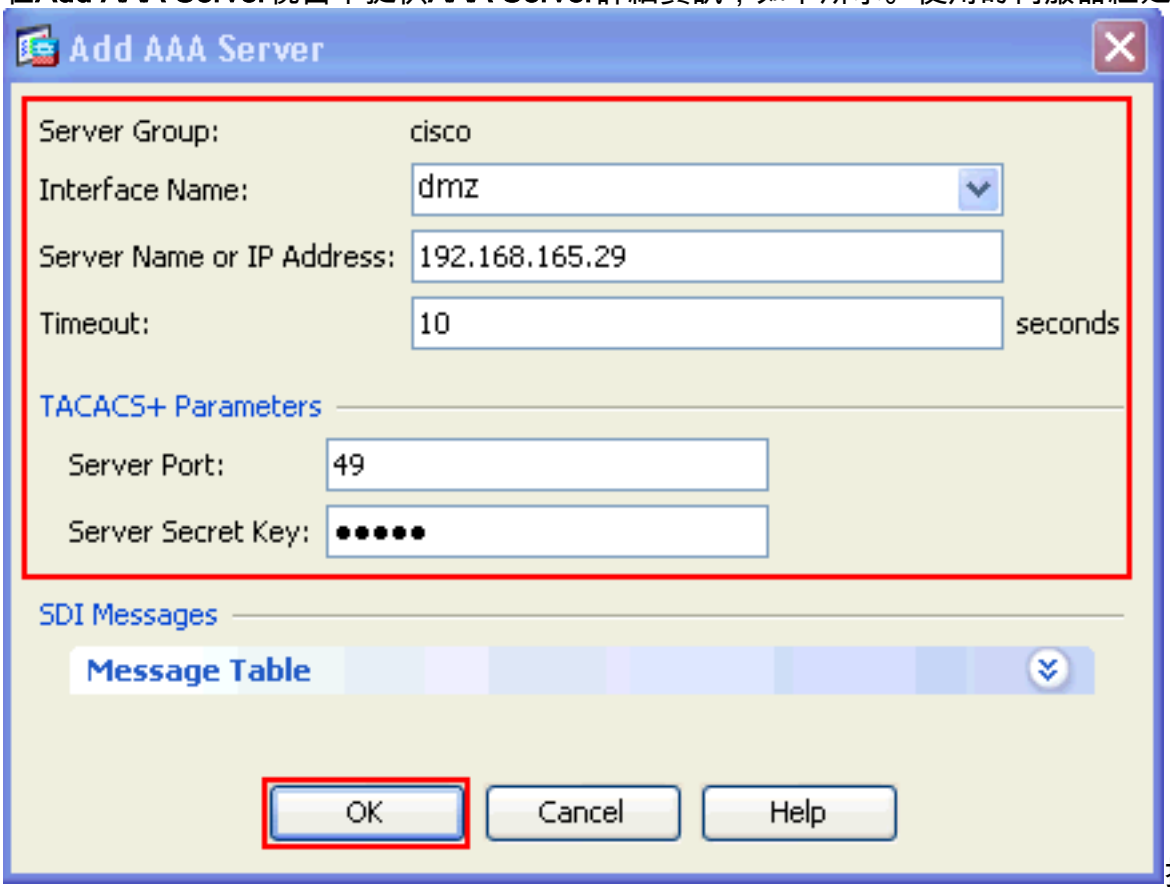


按一下「**OK**」（確定）。

3. 選擇**Configuration > Device Management > Users/AAA > AAA Server Groups**，然後在**Servers in the Selected Group**下按一下**Add**以新增AAA伺服器。

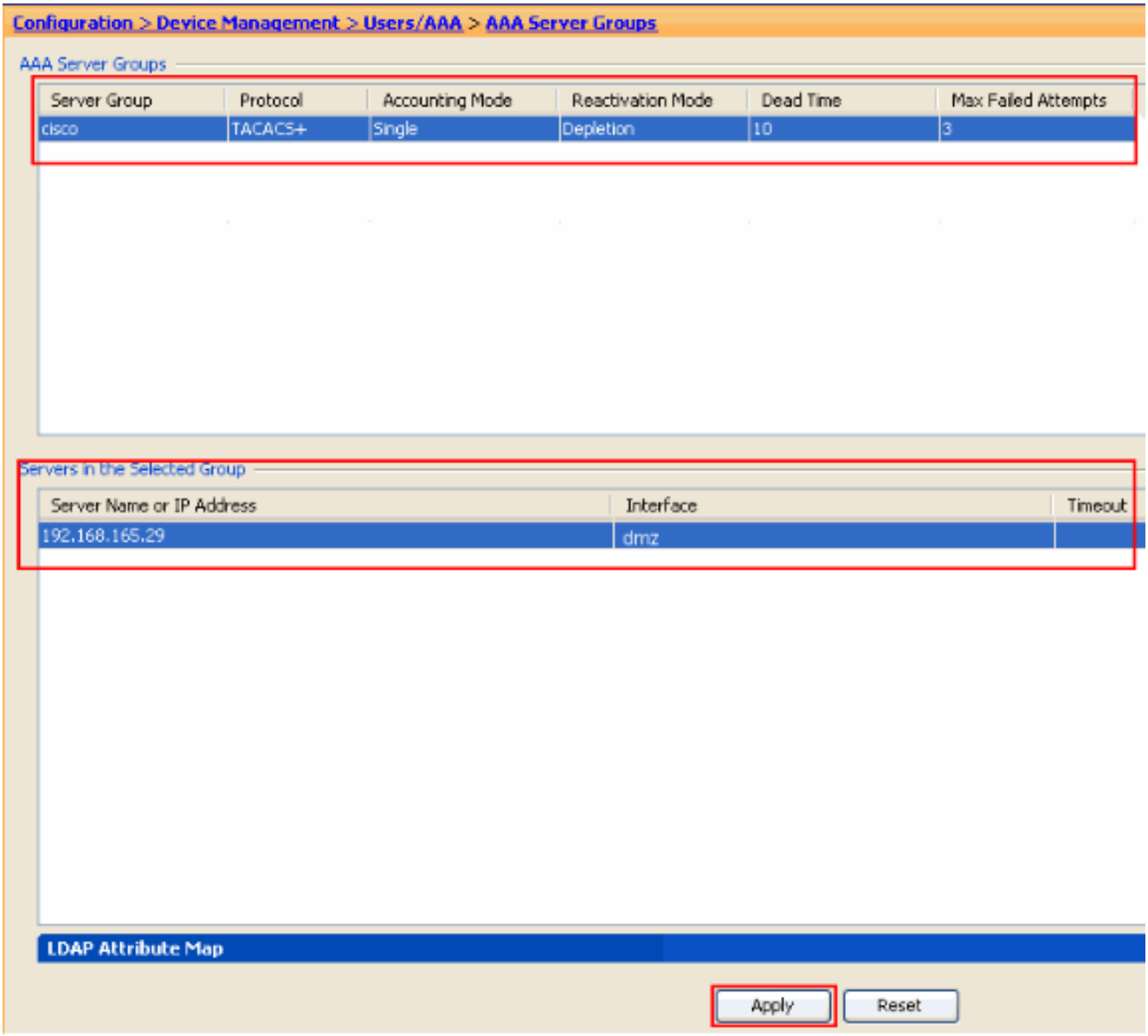


4. 在Add AAA Server視窗中提供AAA Server詳細資訊，如下所示。使用的伺服器組是cisco。

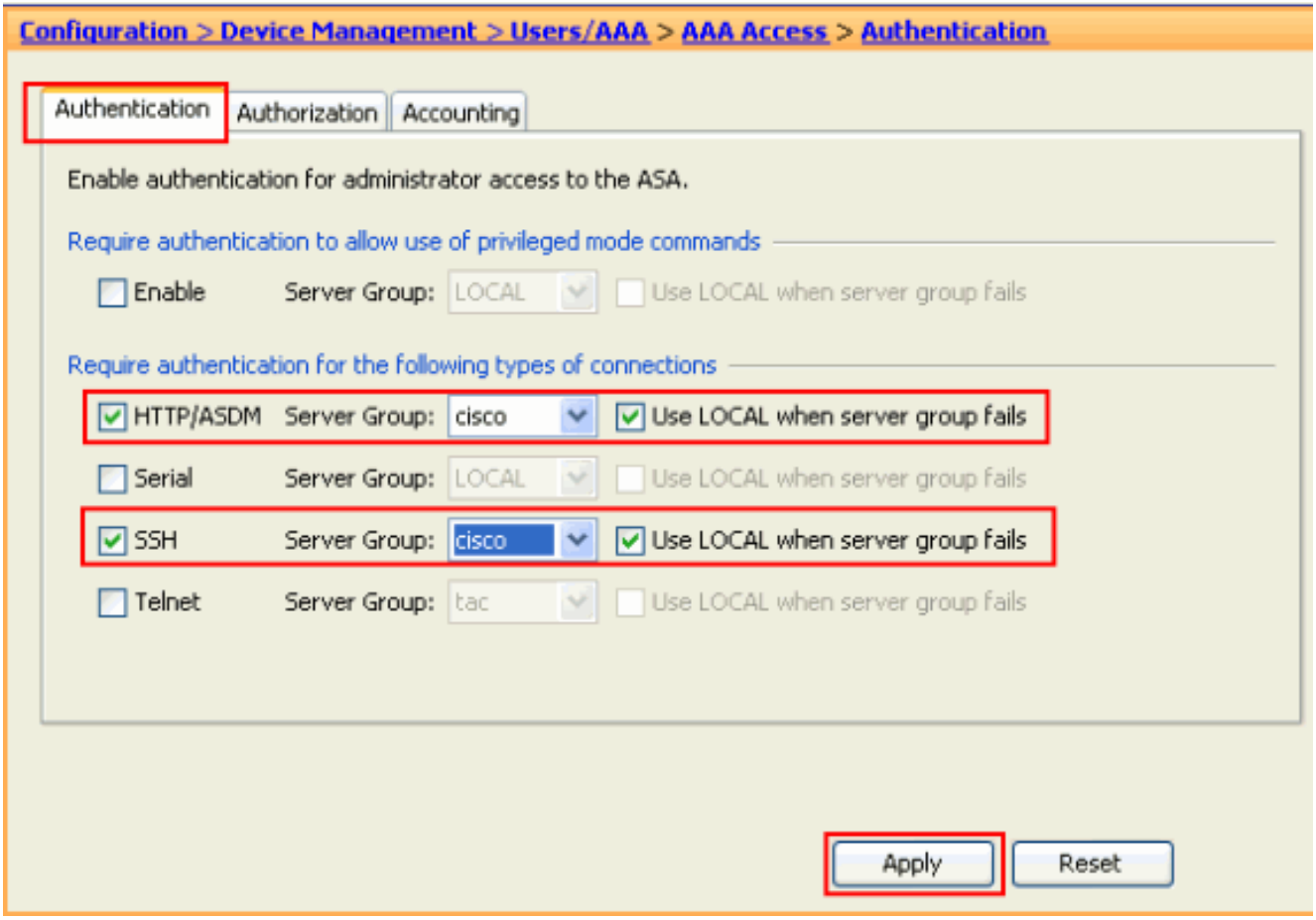


按一下「OK」，然後按一下「Apply」。您將看到AAA Server Group和AAA Server在ASA上配置。

5. 按一下「Apply」。



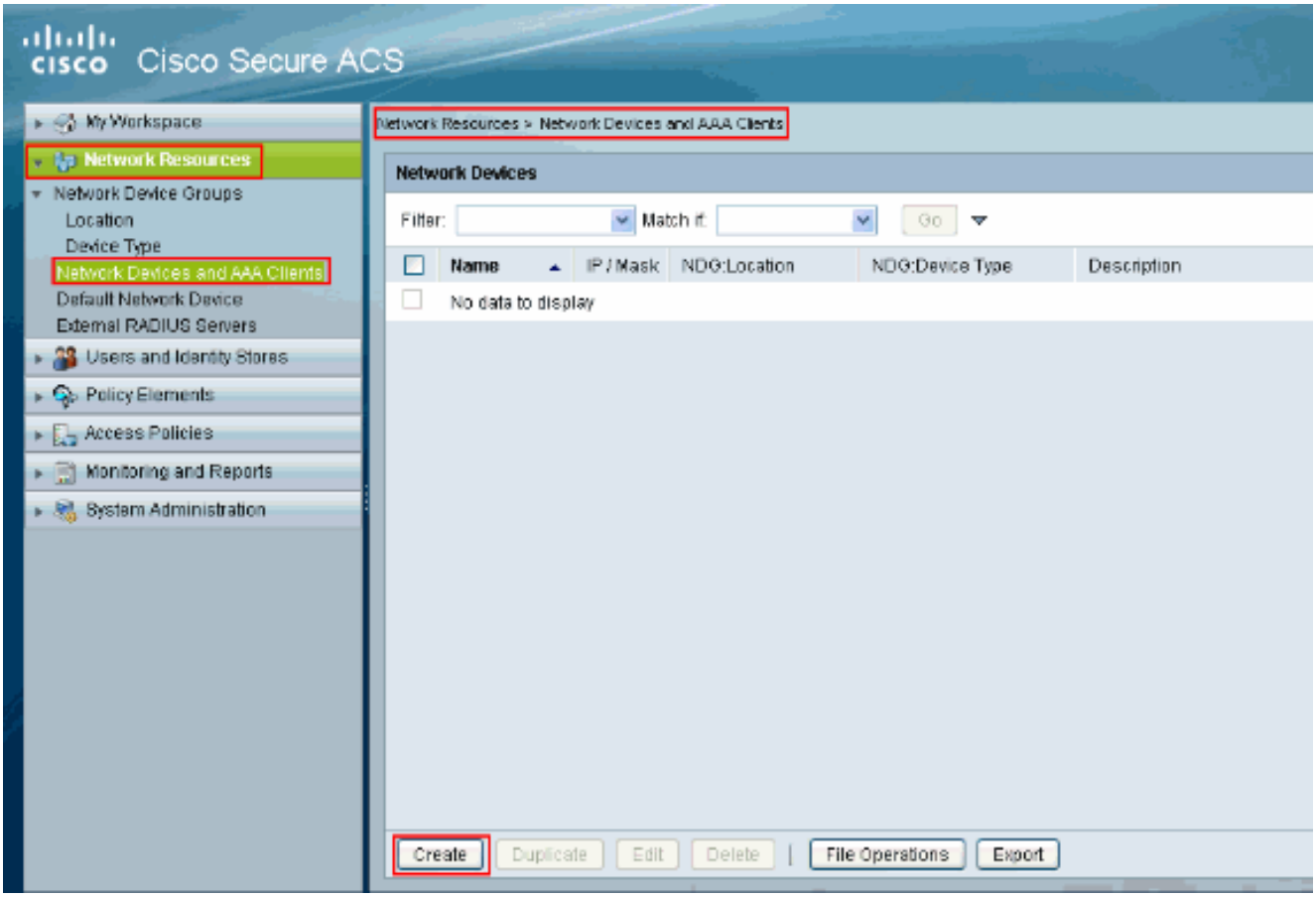
6. 選擇Configuration > Device Management > Users/AAA > AAA Access > Authentication，然後點選HTTP/ASDM和SSH旁邊的覈取方塊。然後選擇cisco作為伺服器組，然後按一下Apply。



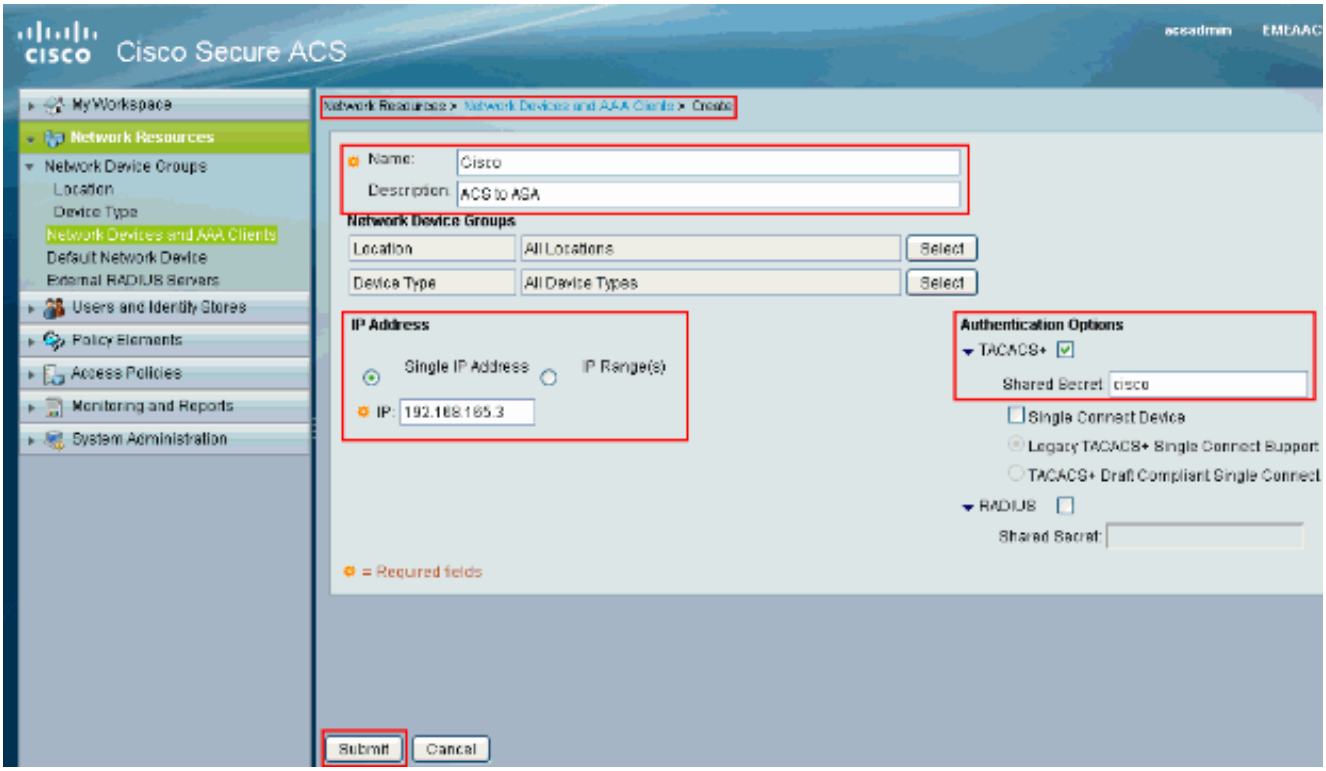
將ACS配置為TACACS伺服器

完成以下步驟即可將ACS配置為TACACS伺服器：

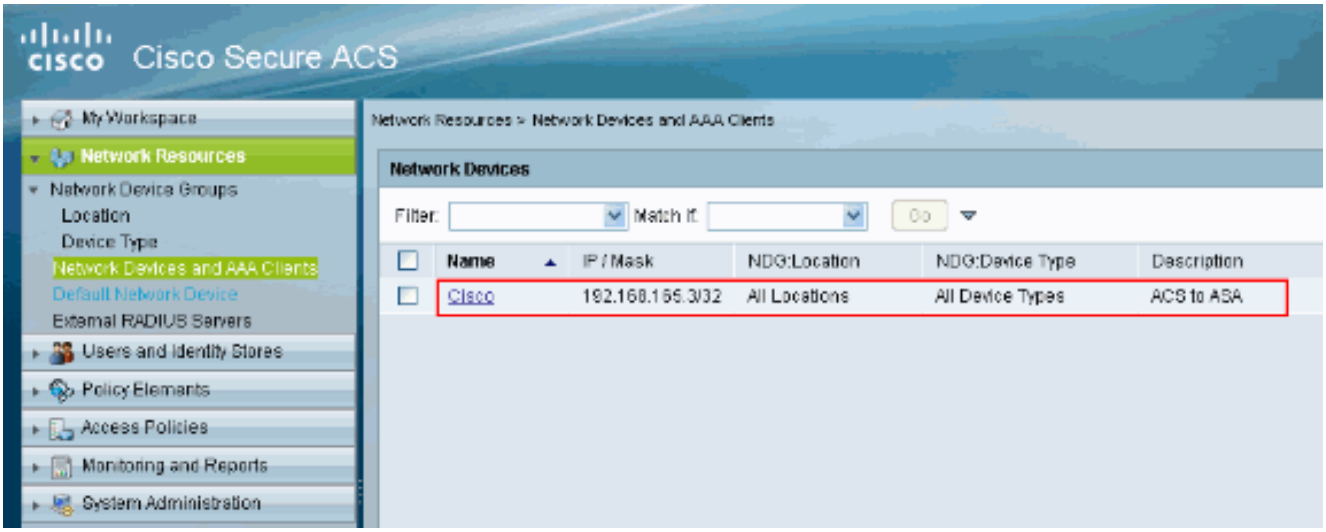
1. 選擇**Network Resources > Network Devices and AAA Clients**，然後按一下**Create**以將ASA新增到ACS伺服器。



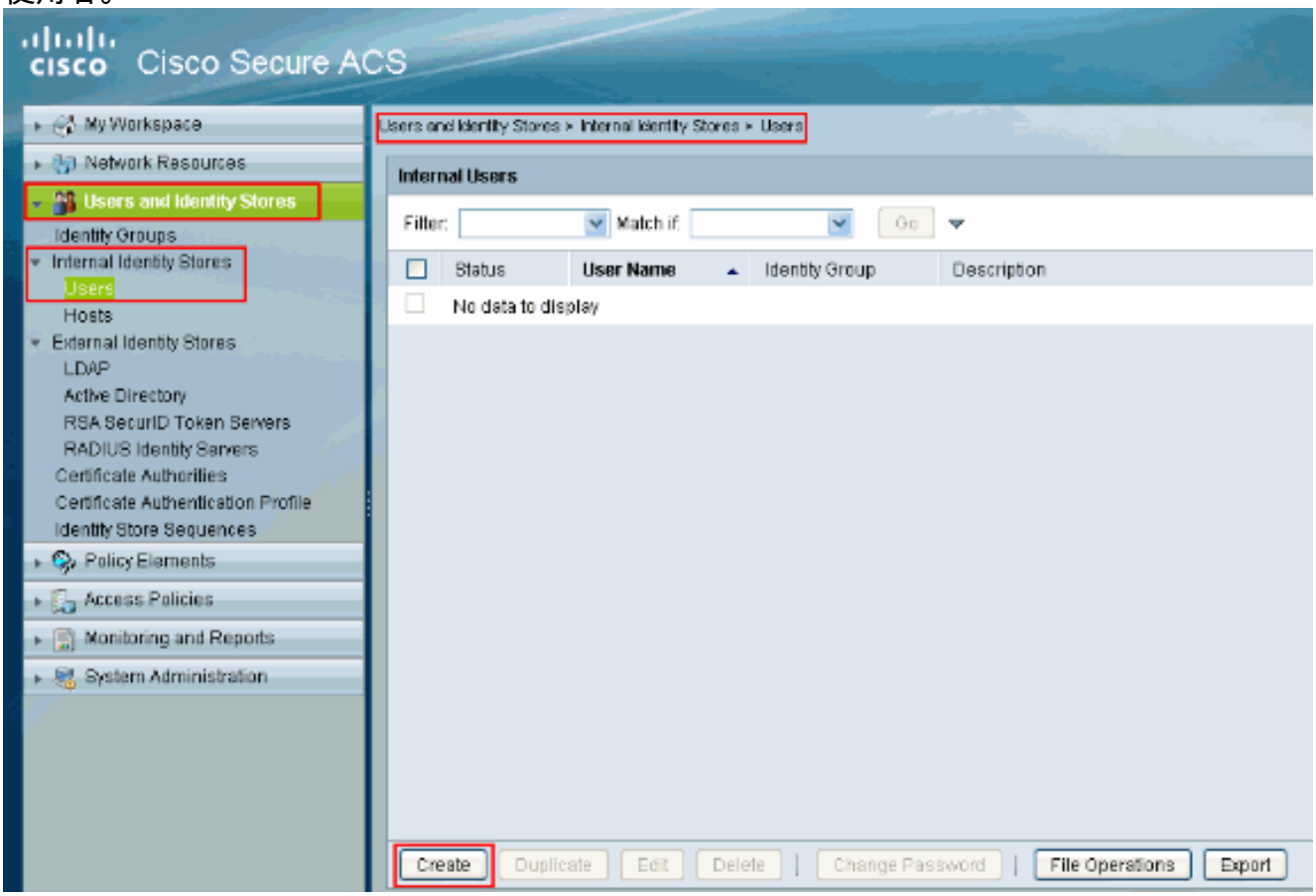
2. 提供有關客戶端的必需資訊(ASA在此為客戶端)，然後按一下**Submit**。這樣可以將ASA新增到ACS伺服器。詳細資訊包括**ASA的**IP地址和TACACS服務**器詳細**資訊。



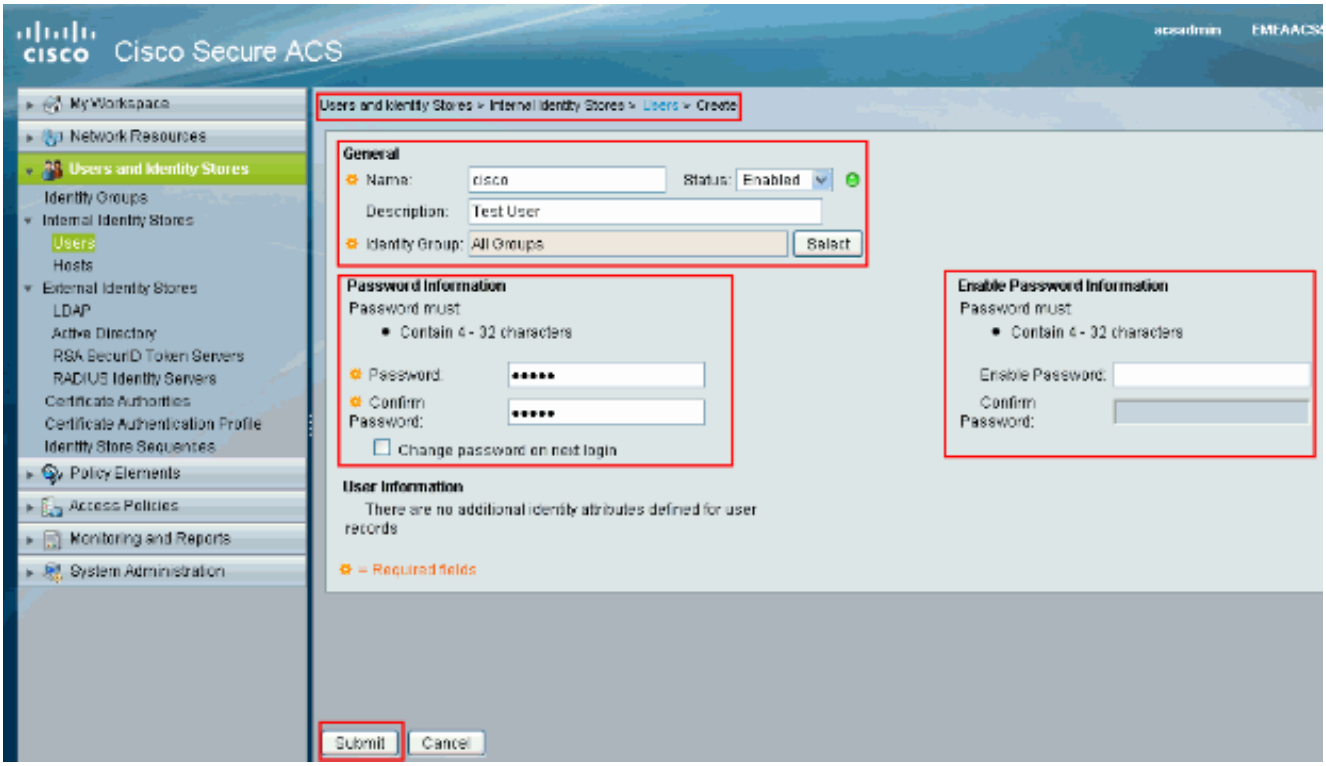
您將看到客戶端**Cisco**被新增到ACS伺服器。



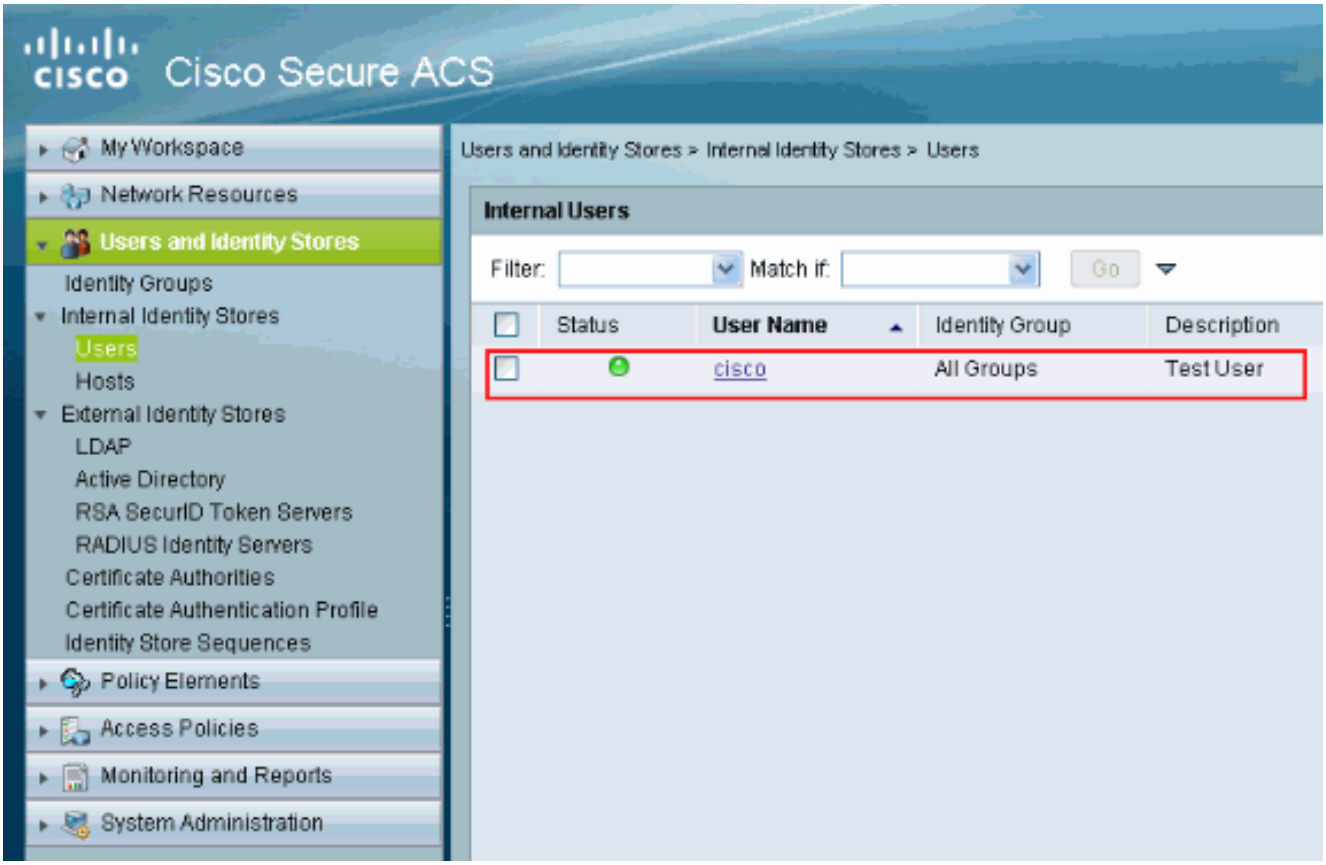
3. 選擇**Users and Identity stores > Internal Identity Stores > Users**，然後按一下**Create**以建立新使用者。



4. 提供名**稱、密碼和啟用密碼**資訊。**啟用密碼**是可**選的**。完成後，按一下**Submit**。



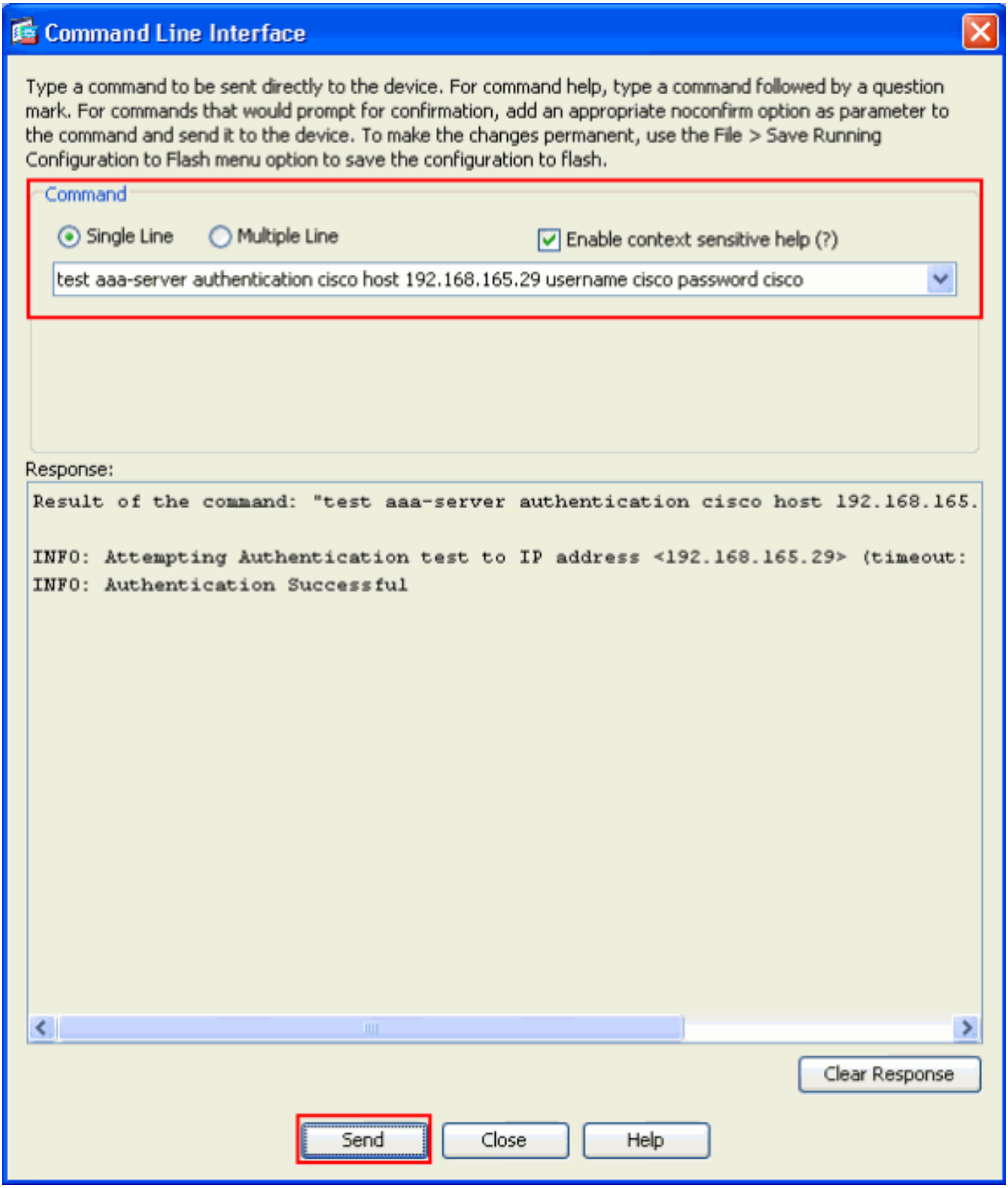
您將看到正在將使用者cisco新增到ACS伺服器。



驗證

使用本節內容，確認您的組態是否正常運作。

使用test aaa-server authentication cisco host 192.168.165.29 username cisco password cisco命令檢查配置是否正常工作。此圖顯示身份驗證成功，並且連線到ASA的使用者已由ACS伺服器進行身份驗證。



輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

疑難排解

錯誤：AAA將AAA伺服器組tacacs中的TACACS+伺服器x.x.x.x標籤為失敗

此消息表示Cisco ASA丟失了與x.x.x.x伺服器的連線。確保tcp 49上從ASA到伺服器x.x.x.x具有有效

的連線。您還可以將TACACS+伺服器的ASA超時從5增加至所需的秒數，以防出現網路延遲。ASA不會向FAILED伺服器x.x.x.x傳送身份驗證請求。但是，它將使用aaa-server組tacacs中的下一個伺服器。

相關資訊

- Cisco ASA 5500系列自適應安全裝置支援頁
- Cisco ASA 5500系列自適應安全裝置命令參考
- 思科調適型資安裝置管理員
- IPsec協商/IKE通訊協定支援頁面
- 思科安全存取控制伺服器（Windows專用）
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems