ASA 8.3：使用ACS 5.X進行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進行身份驗證的資訊。

必要條件

需求

本文檔假定自適應安全裝置(ASA)完全正常運行且已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。

注意：有關如何允許ASDM遠端配置裝置的詳細資訊，請參閱允許對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。

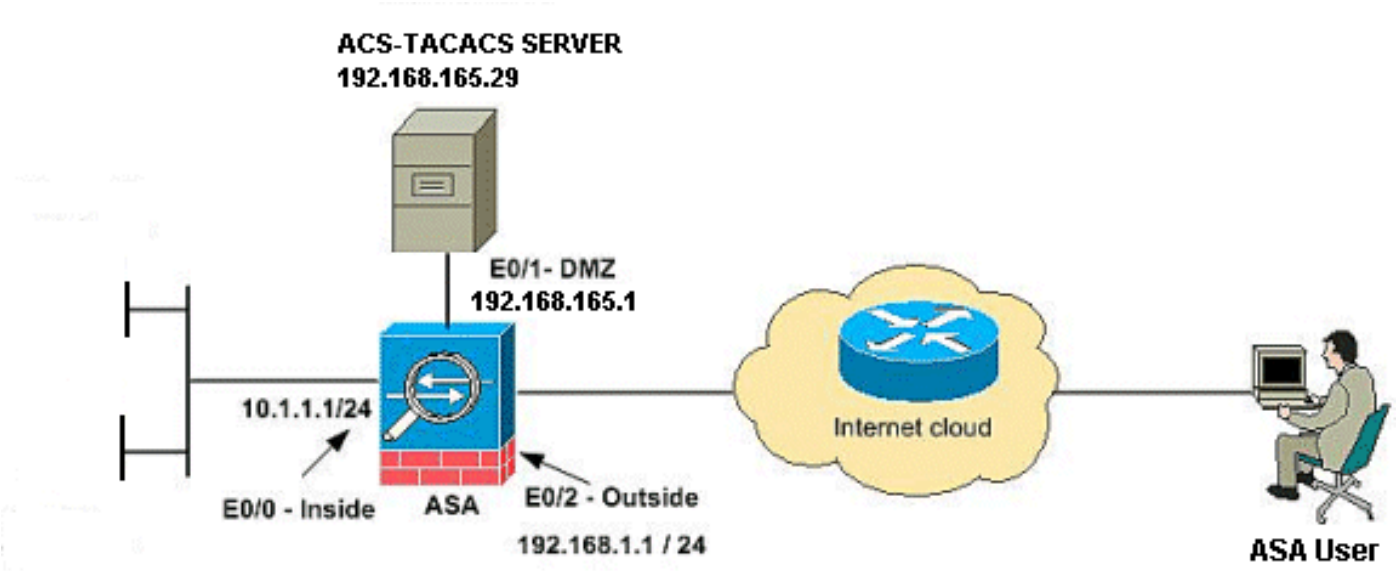
設定

本節提供用於設定本文件中所述功能的資訊。

注意：使用命令查詢工具(僅限註冊客戶)可以獲取有關本部分使用的命令的更多資訊。

網路圖表

此文件使用以下網路設定：



注意：此配置中使用的IP編址方案在Internet上無法合法路由。這些地址是在實驗室環境中使用的RFC 1918地址。

使用CLI配置從ACS伺服器進行身份驗證的ASA

為ASA執行以下配置，以便從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
```

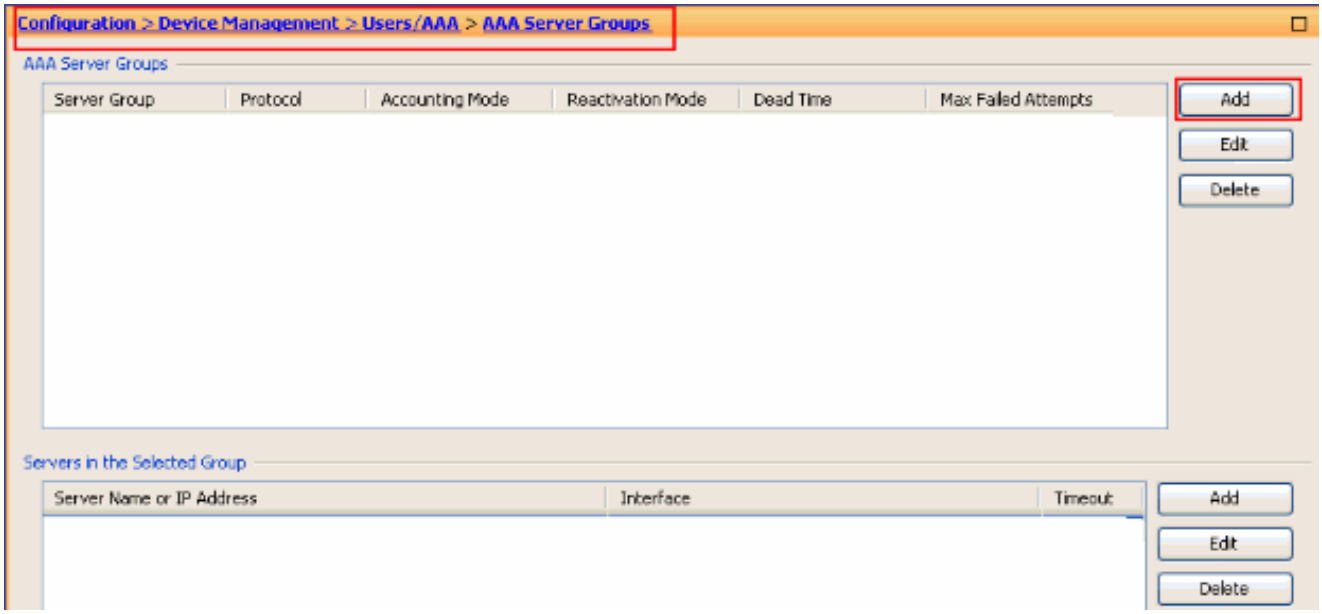
注意：當ACS不可用時，在ASA上使用username cisco password cisco privilege 15 命令建立一個本地使用者以使用本地身份驗證訪問ASDM。

使用ASDM配置用於從ACS伺服器進行身份驗證的ASA

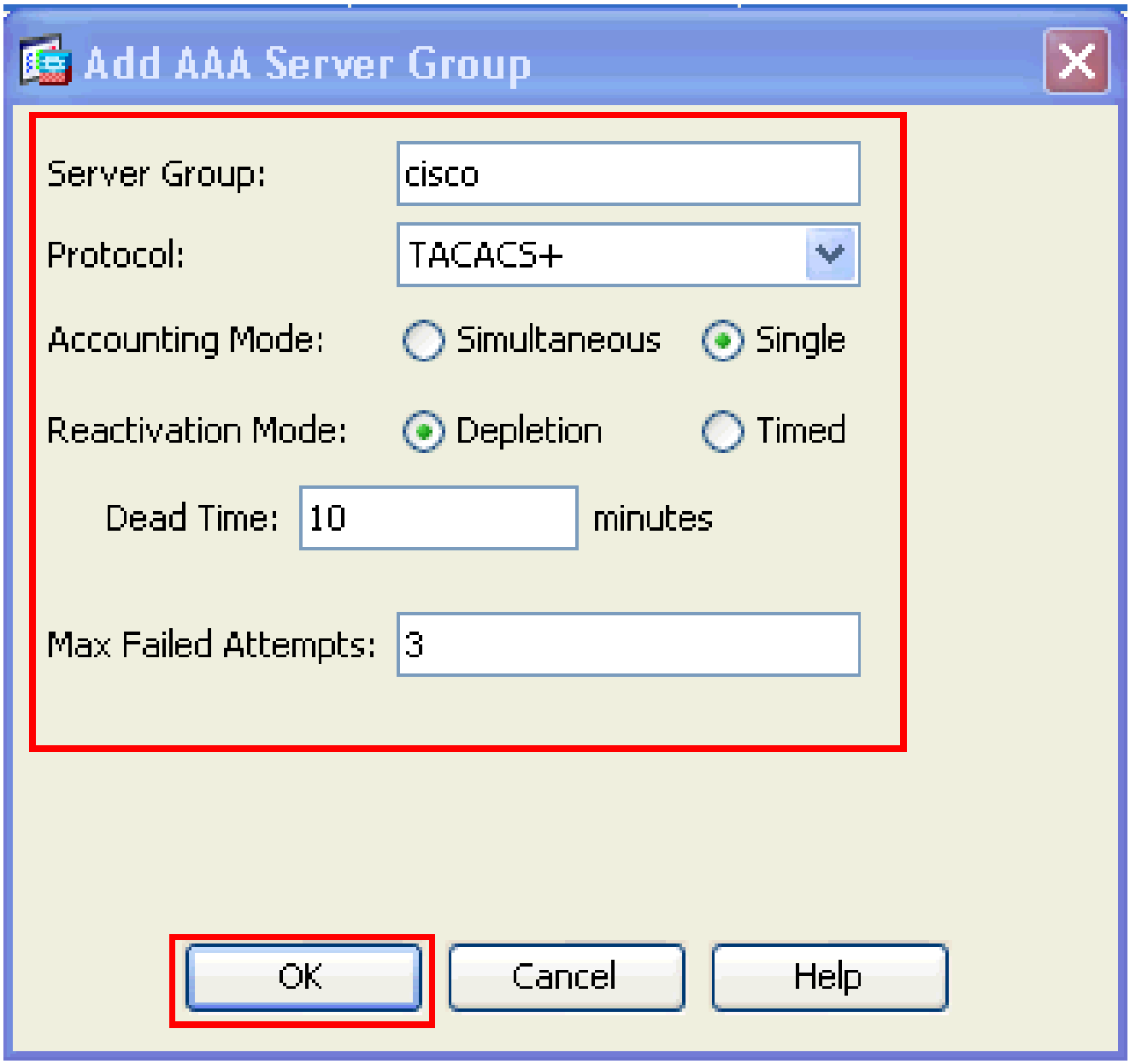
ASDM過程

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。

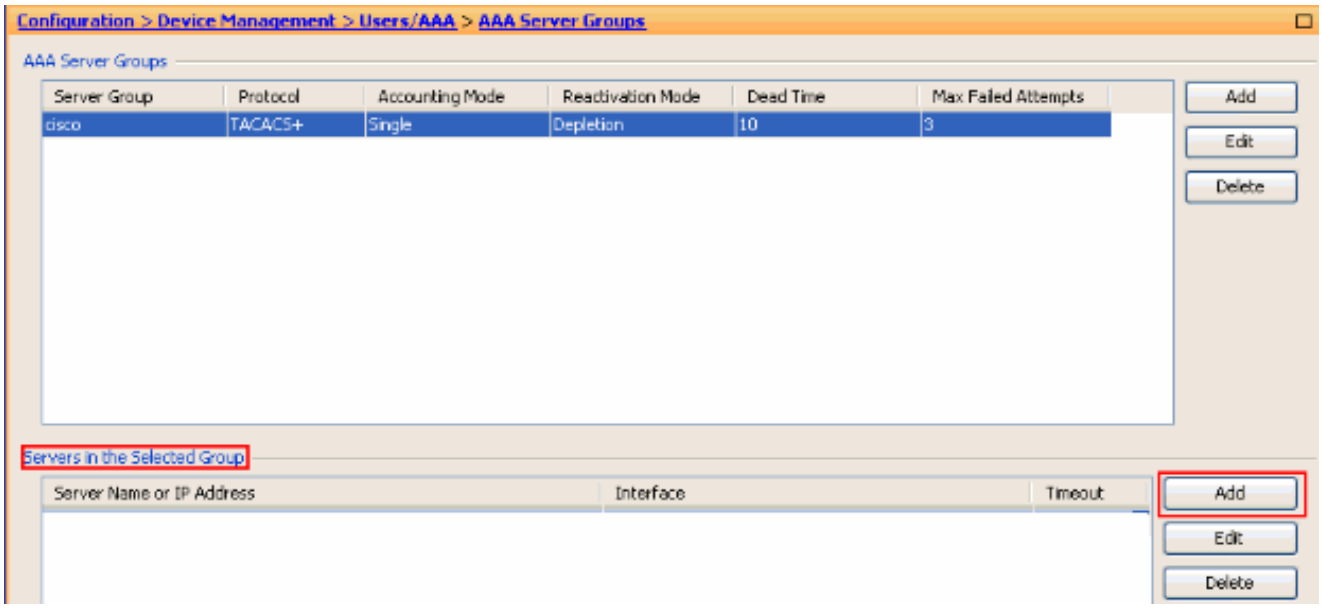


2. 在Add AAA Server Group窗口中提供AAA Server Group詳細資訊，如下所示。使用的協定是TACACS+，並且建立的伺服器組是cisco。

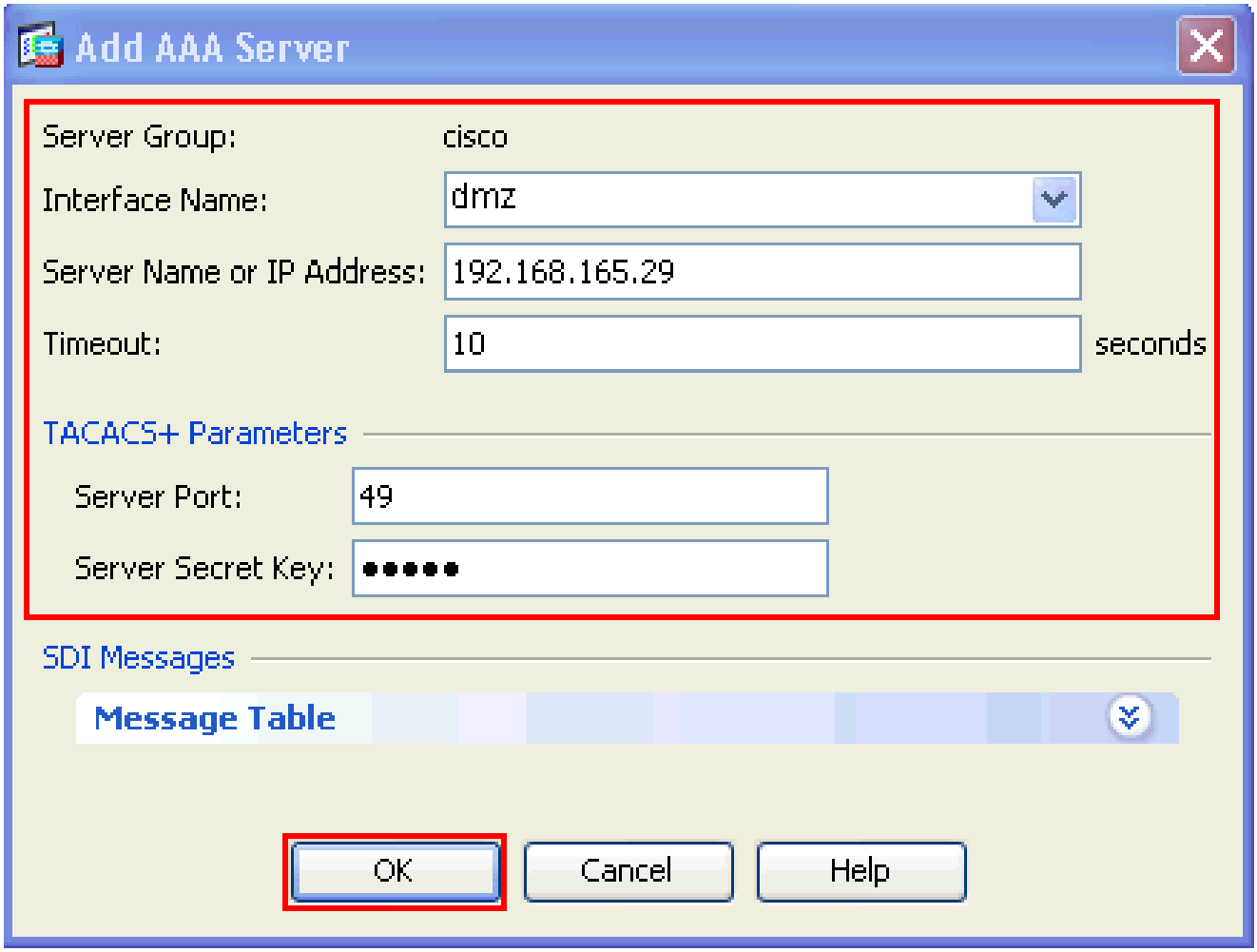


按一下「OK」（確定）。

3. 選擇Configuration > Device Management > Users/AAA > AAA Server Groups，然後按一下Servers in the Selected Group下的Add以增加AAA伺服器。



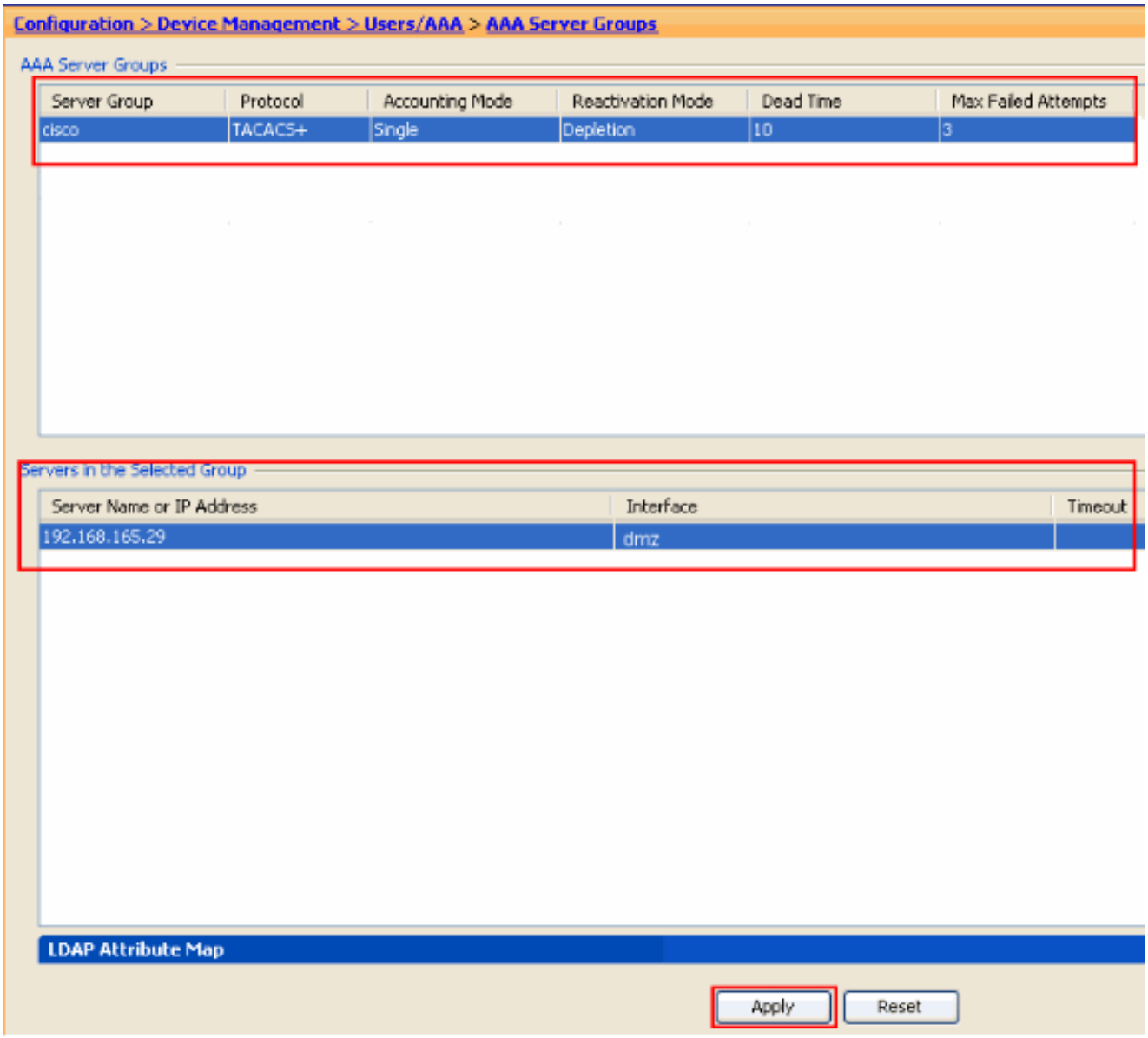
4. 在Add AAA Server窗口中提供AAA Server詳細資訊，如下所示。使用的伺服器組是cisco。



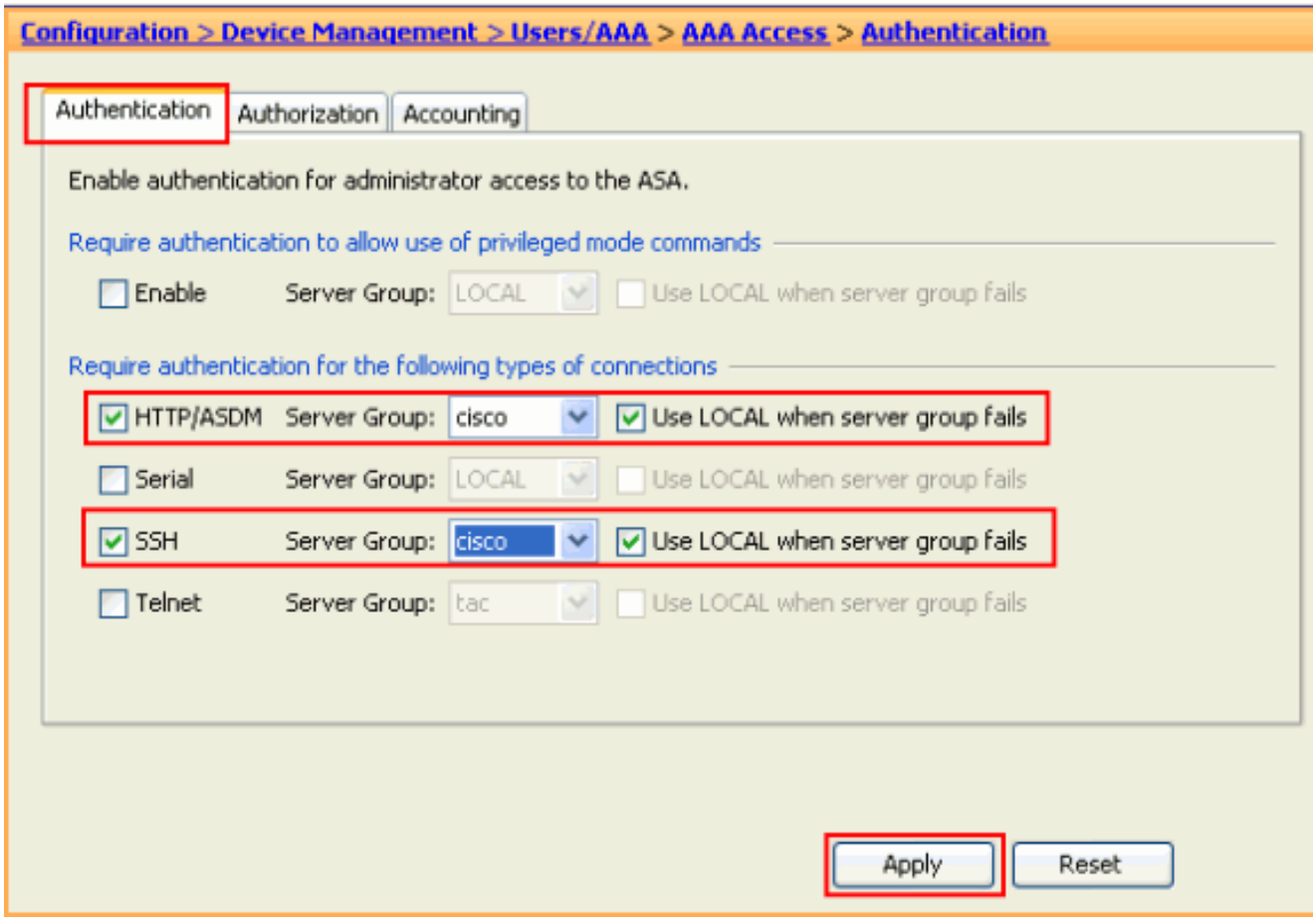
按一下OK，然後按一下Apply。

您將看到ASA上配置了AAA伺服器組和AAA伺服器。

5. 按一下「Apply」。



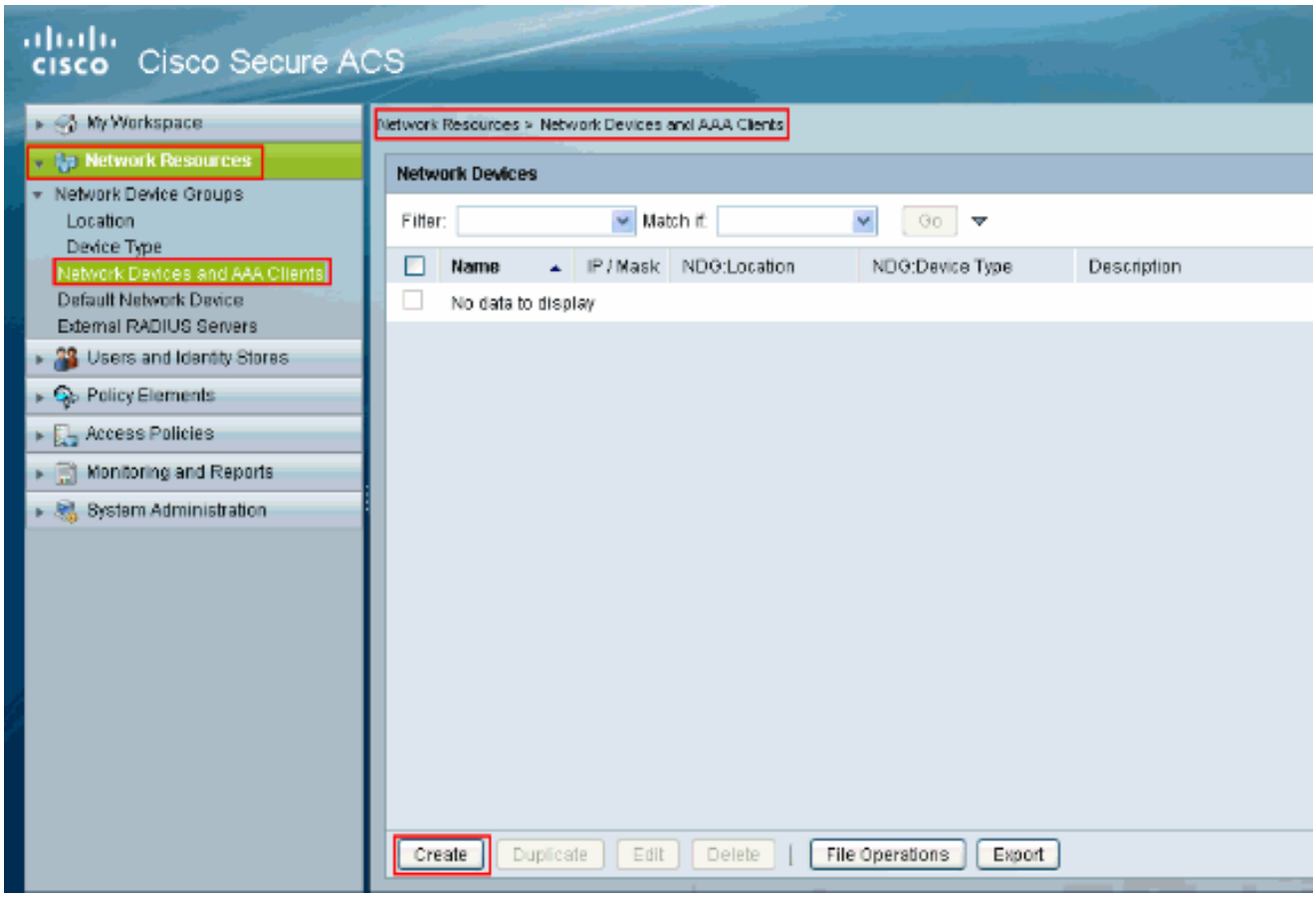
6. 選擇Configuration > Device Management > Users/AAA > AAA Access > Authentication，然後按一下HTTP/ASDM和SSH旁邊的覈取方塊。然後，選擇cisco作為伺服器組並按一下Apply。



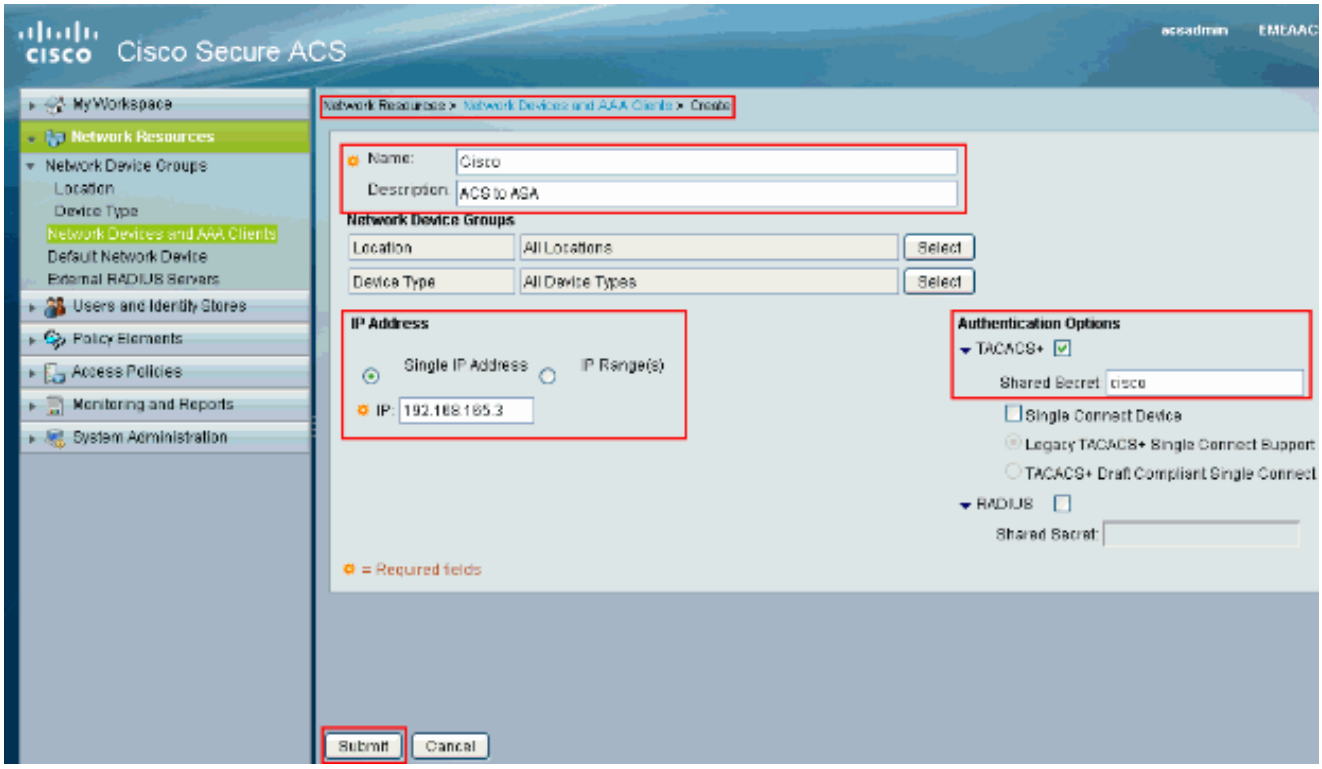
將ACS配置為TACACS伺服器

要將ACS配置為TACACS伺服器，請完成以下步驟：

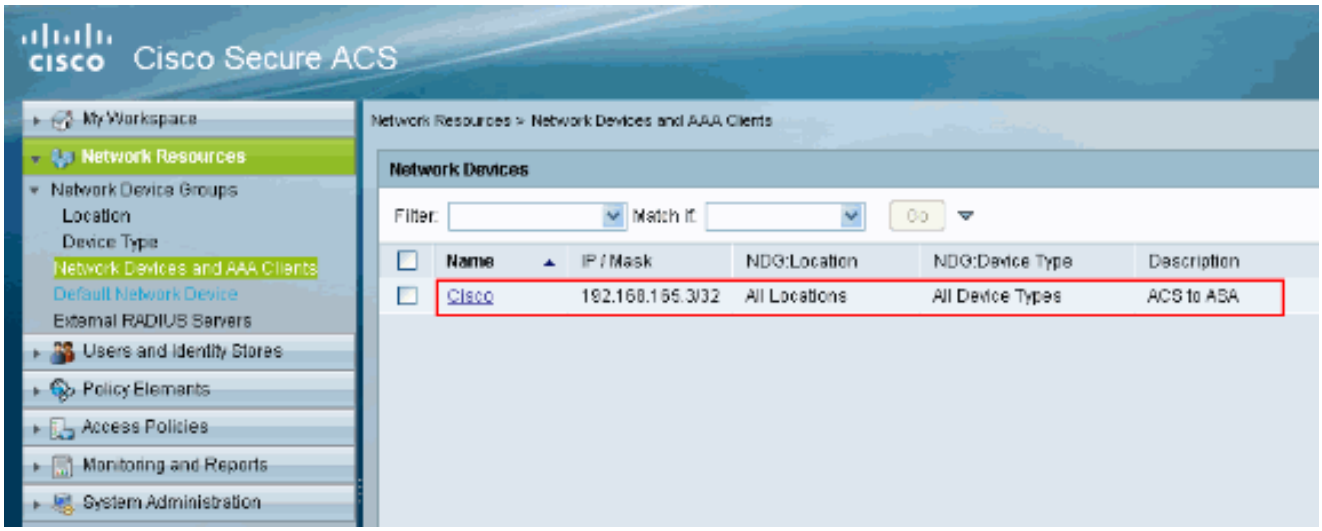
1. 選擇Network Resources > Network Devices and AAA Clients並按一下Create，以便將ASA增加到ACS伺服器。



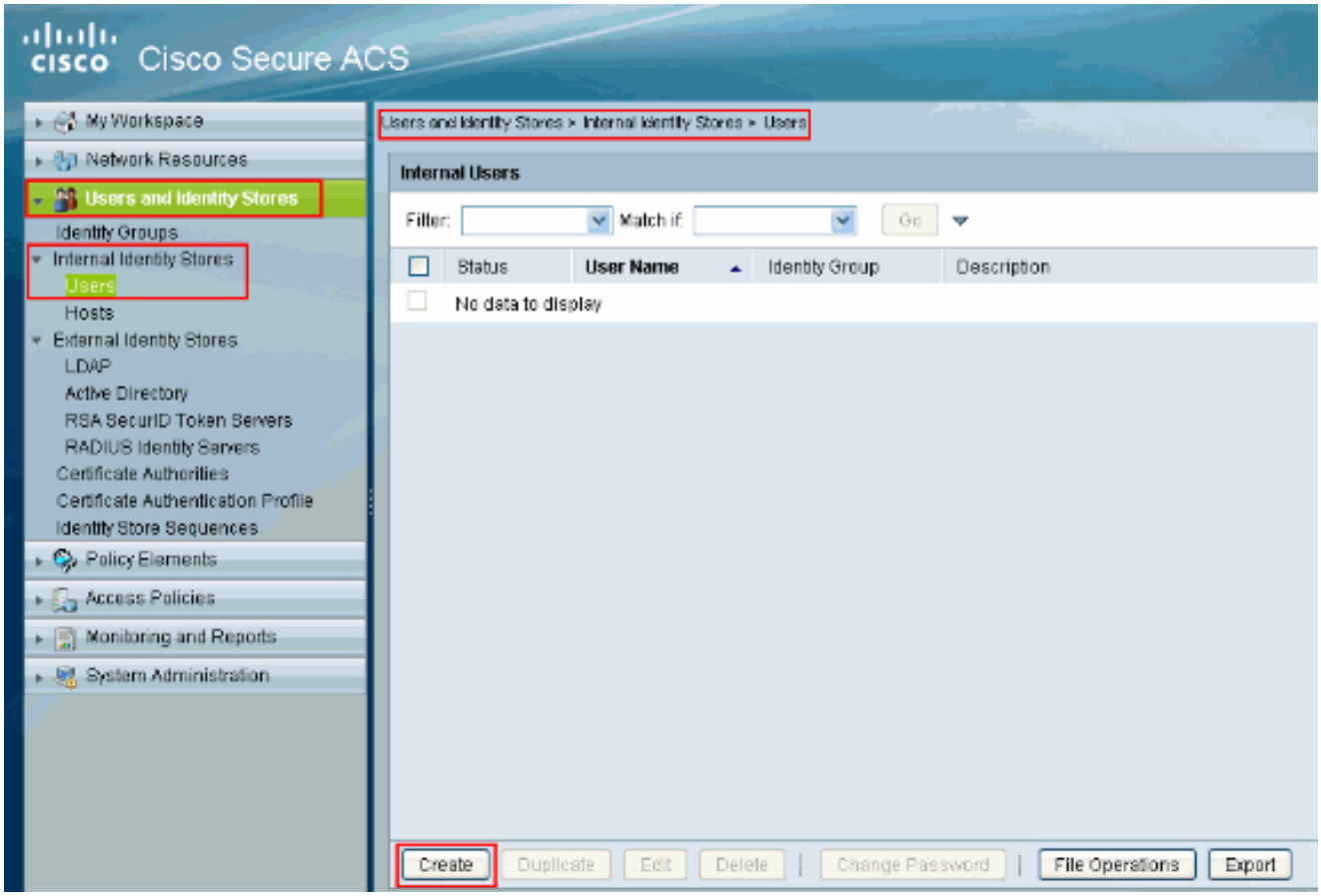
2. 提供有關客戶端（此處的ASA是客戶端）的必要資訊，然後按一下Submit。這使ASA能夠增加到ACS伺服器。詳細資訊包括ASA的IP地址和TACACS伺服器詳細資訊。



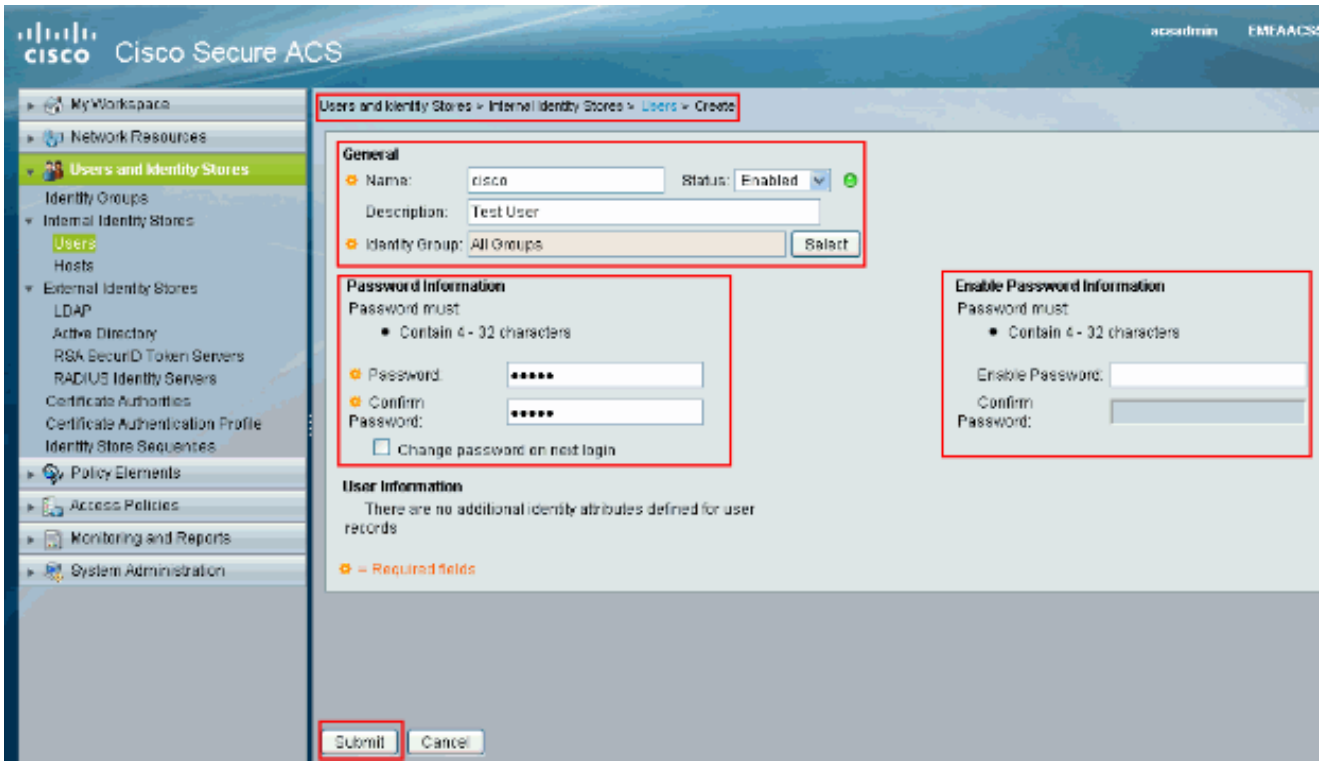
您將看到客戶端Cisco被增加到ACS伺服器。



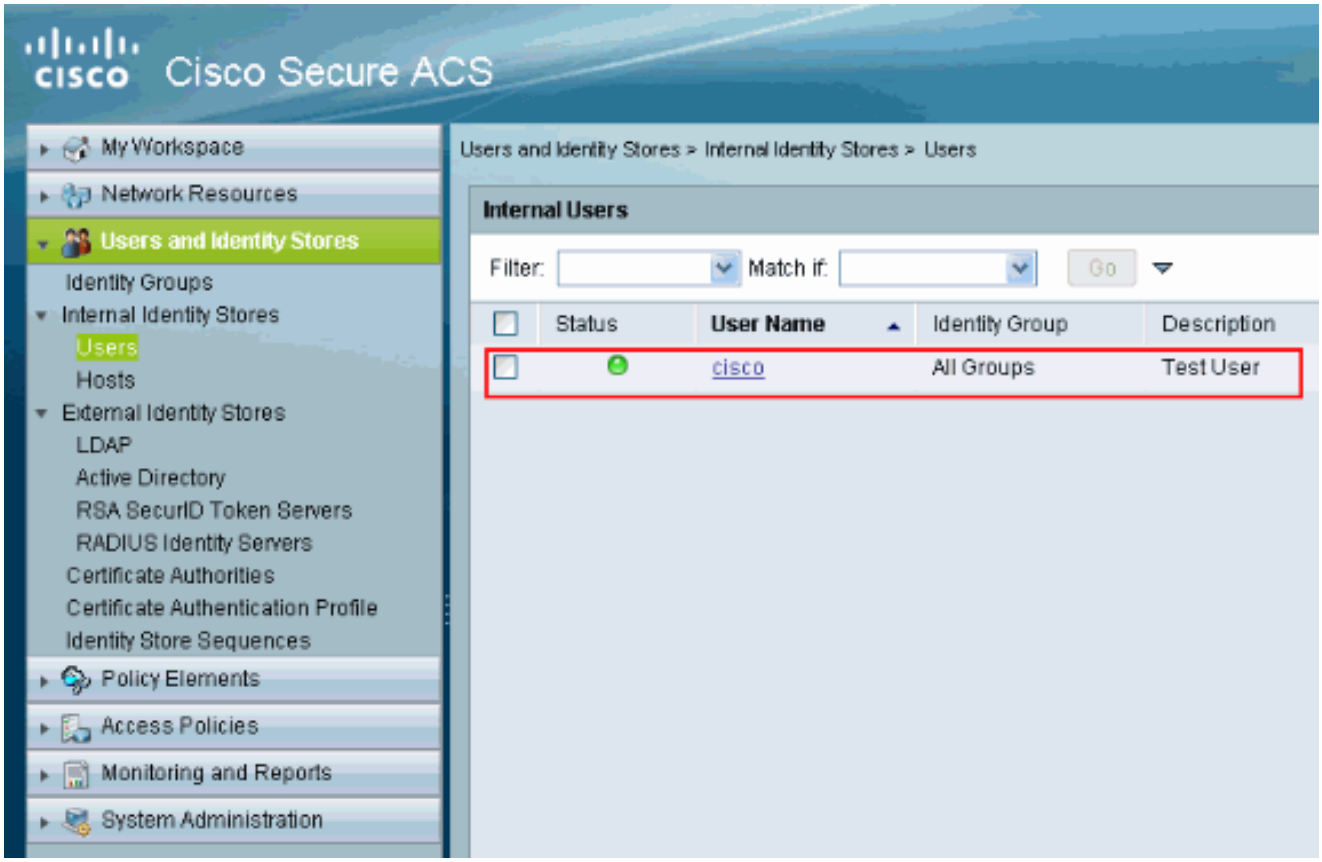
3. 選擇Users and Identity stores > Internal Identity Stores > Users，然後按一下Create以建立新使用者。



4. 提供名稱、密碼和啟用密碼資訊。Enable Password為可選。當您完成時，按一下Submit。



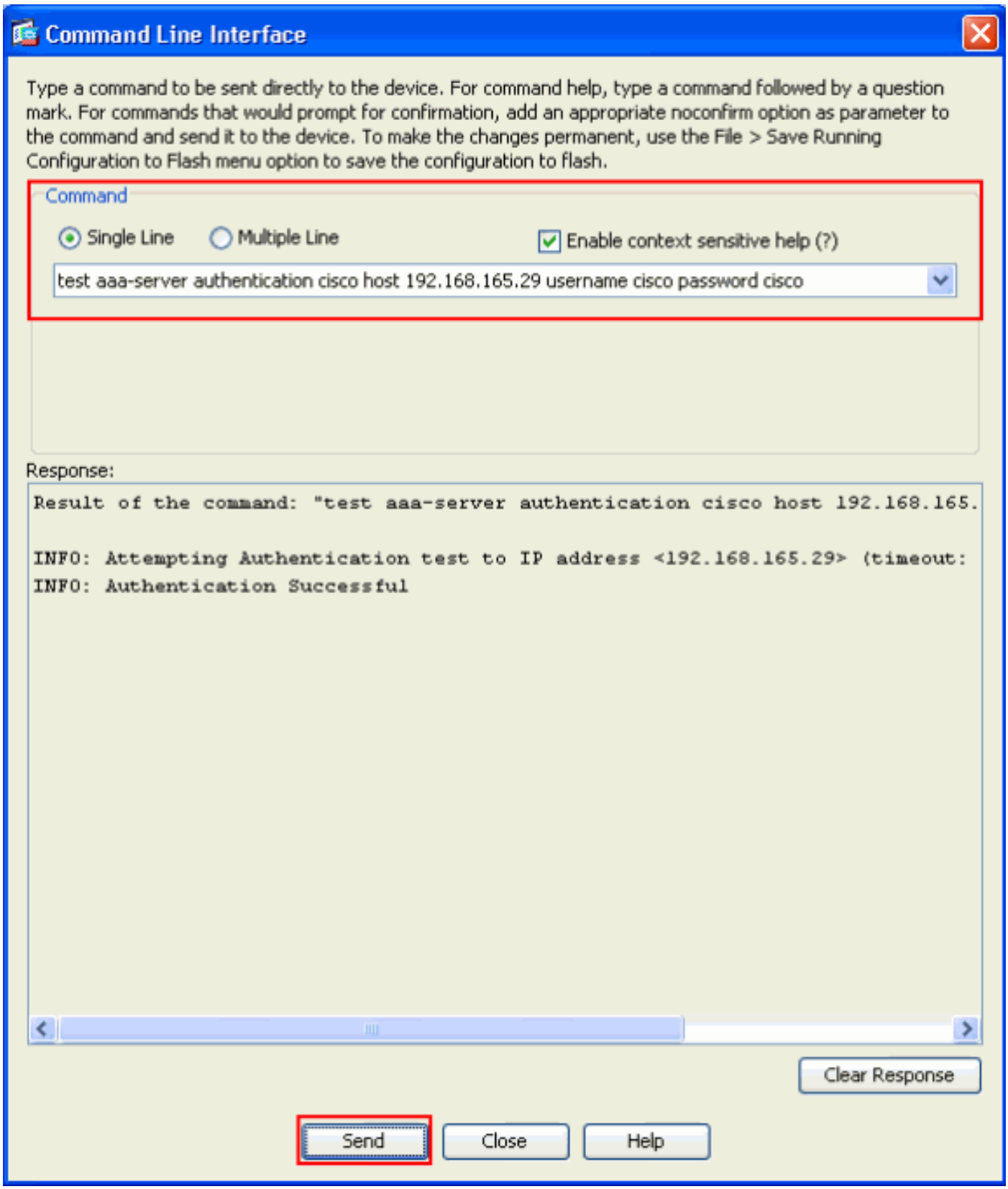
您將看到使用者cisco被增加到ACS伺服器。



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的使用者已透過ACS伺服器的身份驗證。



輸出直譯器工具(僅供註冊客戶使用) (OIT)支援某些show指令。使用OIT檢視對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失去與x.x.x.x伺服器的連線。確保您在tcp 49上擁有從ASA到伺服器x.x.x.x的有效連線。您還可以將TACACS+伺服器的ASA超時從5增加到所需的秒數，以防出現網路延遲。ASA不會向失敗伺服器x.x.x.x傳送身份驗證請求。但是，它將使用aaa-server組tacacs中的下一台伺服器。

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
- 適用於Windows的Cisco安全存取控制伺服器
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。