ASA 8.3:ACS 5.X를 사용한 TACACS 인증

목차

소개

이 문서에서는 네트워크 액세스를 위해 사용자를 인증하도록 보안 어플라이언스를 구성하는 방법에 대한 정보를 제공합니다.

사전 요구 사항

요구 사항

이 문서에서는 ASA(Adaptive Security Appliance)가 완벽하게 작동하며 Cisco ASDM(Adaptive Security Device Manager) 또는 CLI에서 컨피그레이션을 변경할 수 있도록 구성되어 있다고 가정합니다.

참고: ASDM에서 디바이스를 원격으로 구성하는 방법에 대한 자세한 내용은 ASDM용 HTTPS 액세스 허용 을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Adaptive Security Appliance Software 버전 8.3 이상
- Cisco Adaptive Security Device Manager 버전 6.3 이상
- Cisco Secure Access Control Server 5.x

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

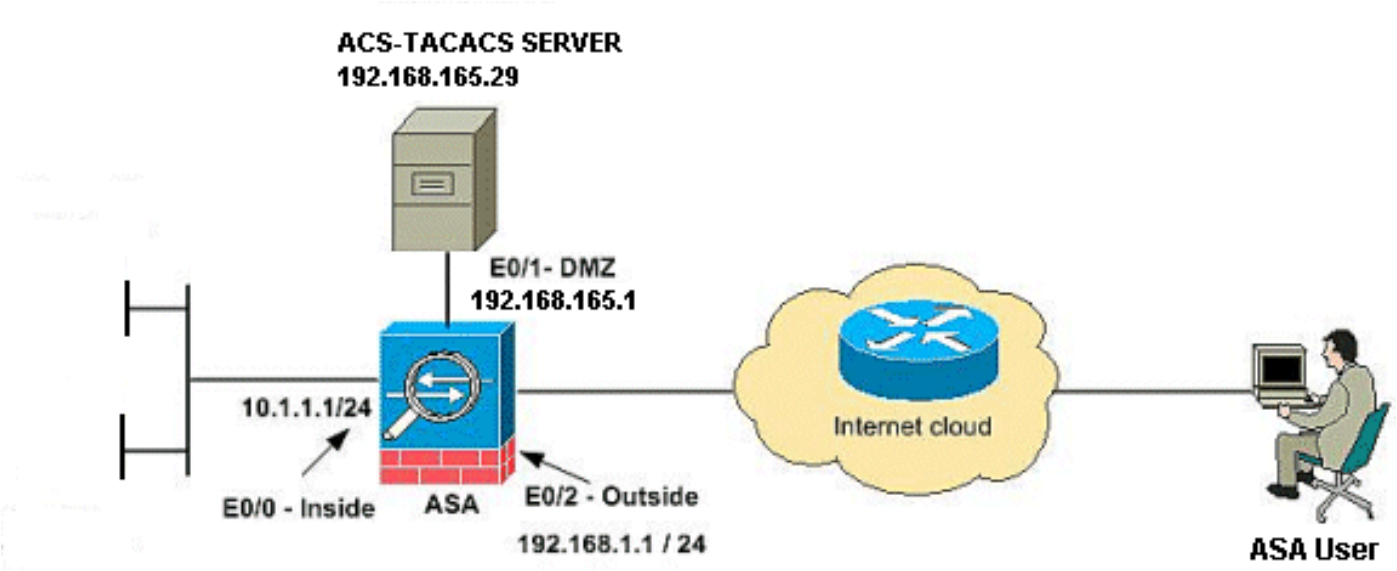
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 명령 조회 도구(등록된 고객만 해당)를 사용하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.실습 환경에서 사용된 RFC 1918 주소입니다.

CLI를 사용하여 ACS 서버에서 인증을 위한 ASA 구성

ASA에 대해 다음 컨피그레이션을 수행하여 ACS 서버에서 인증합니다.

```
!--- 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
```

참고: ACS를 사용할 수 없을 때 로컬 인증을 사용하여 ASDM에 액세스하려면 사용자 이름 cisco

password cisco privilege 15 명령을 사용하여 ASA에서 로컬 사용자를 생성합니다.

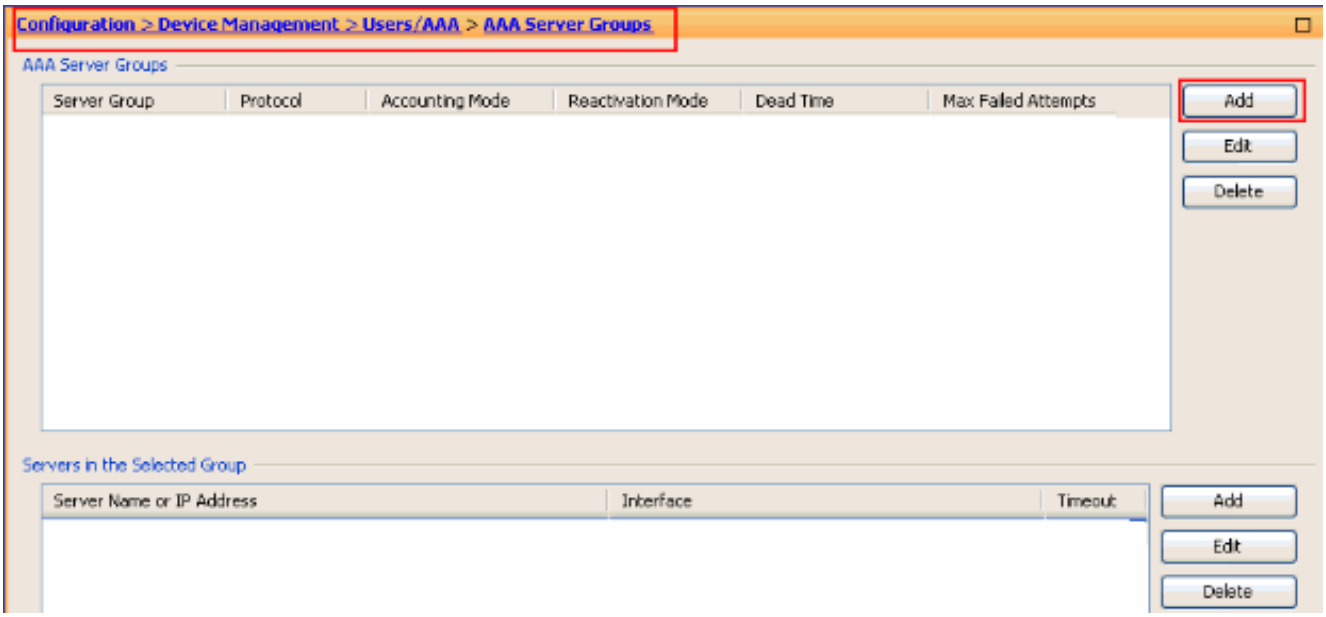
ASDM을 사용하여 ACS 서버에서 인증을 위한 ASA 구성

ASDM 절차

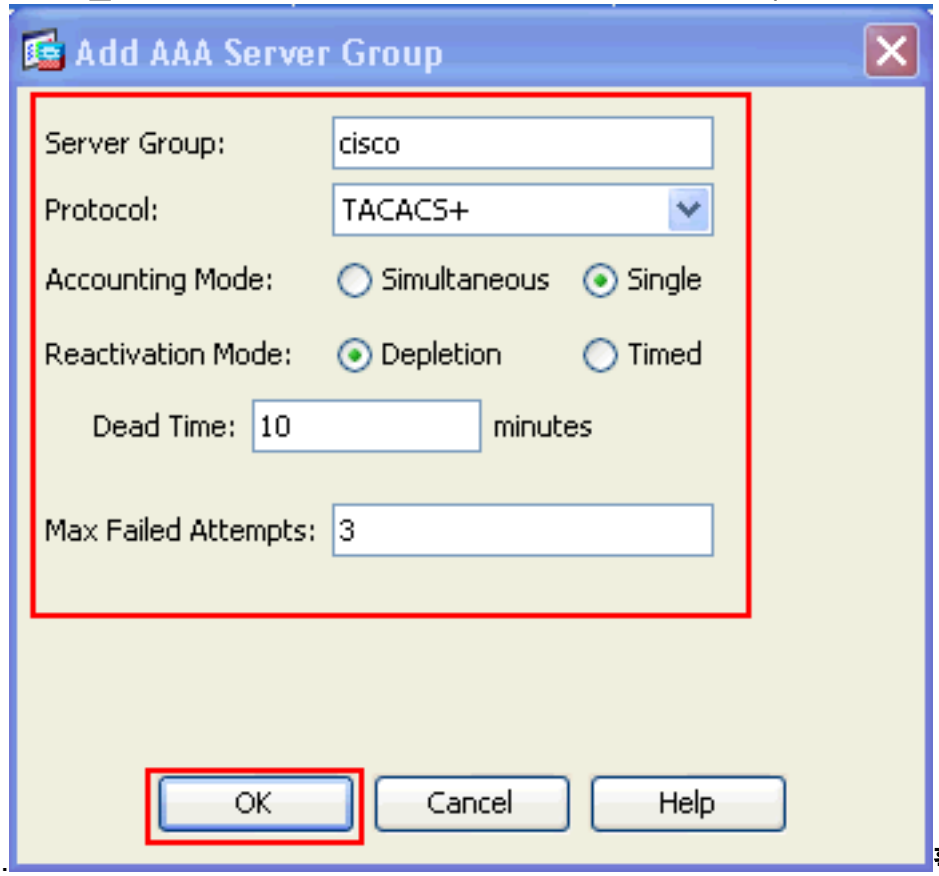
ACS 서버에서 인증을 위해 ASA를 구성하려면 다음 단계를 완료합니다.

1. AAA 서버 그룹을 생성하려면 Configuration > Device Management > Users/AAA > AAA Server Groups > Add를 선택합니다

.



2. 표시된 대로 Add AAA Server Group(AAA 서버 그룹 추가) 창에서 AAA Server Group(AAA 서버 그룹) 세부사항을 제공합니다.사용되는 프로토콜은 TACACS+이며 생성된 서버 그룹은 cisco입니다.

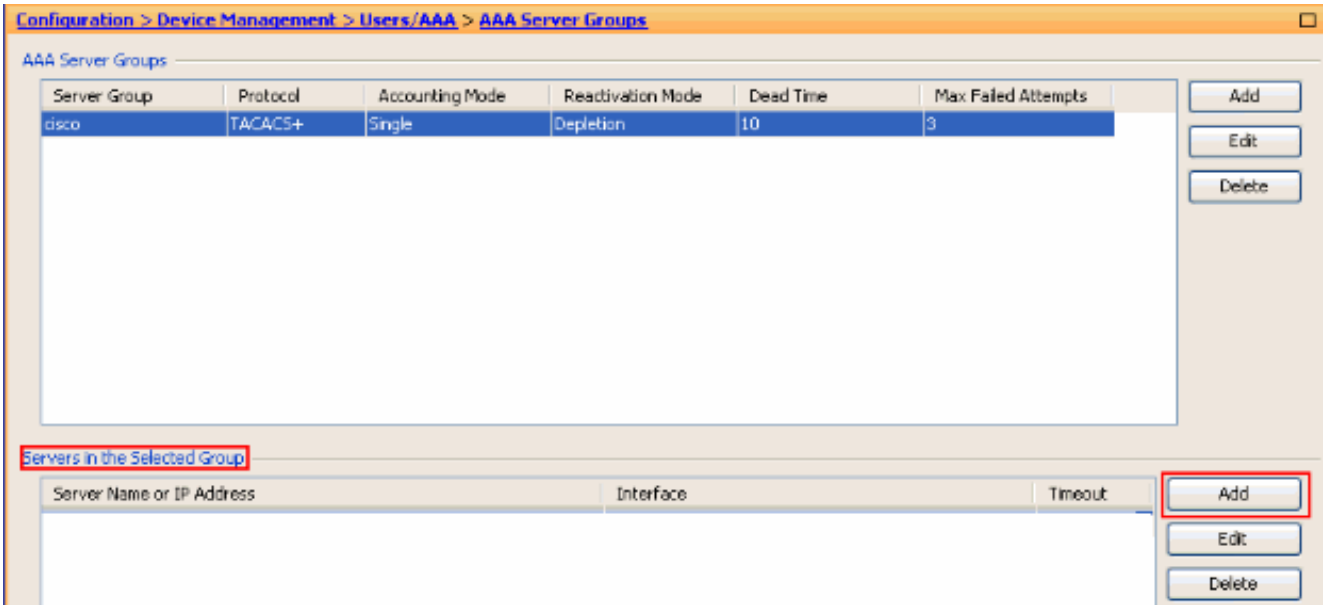


확인을 클릭합

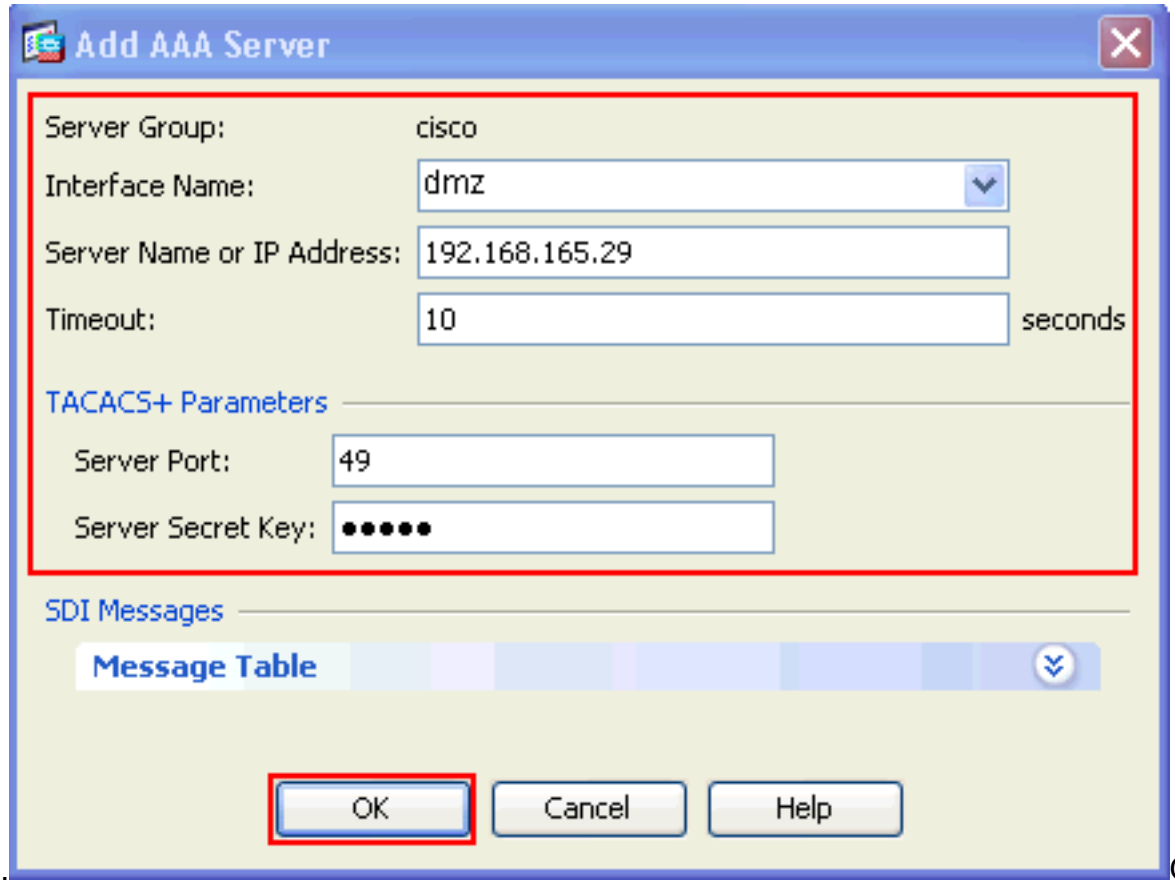
니다.

3. Configuration **> Device Management > Users/AAA > AAA Server Groups**를 선택하고 Selected Group의 **Servers** 아래**에서 Add**를 클릭하여 AAA 서버를 추가합니다

.



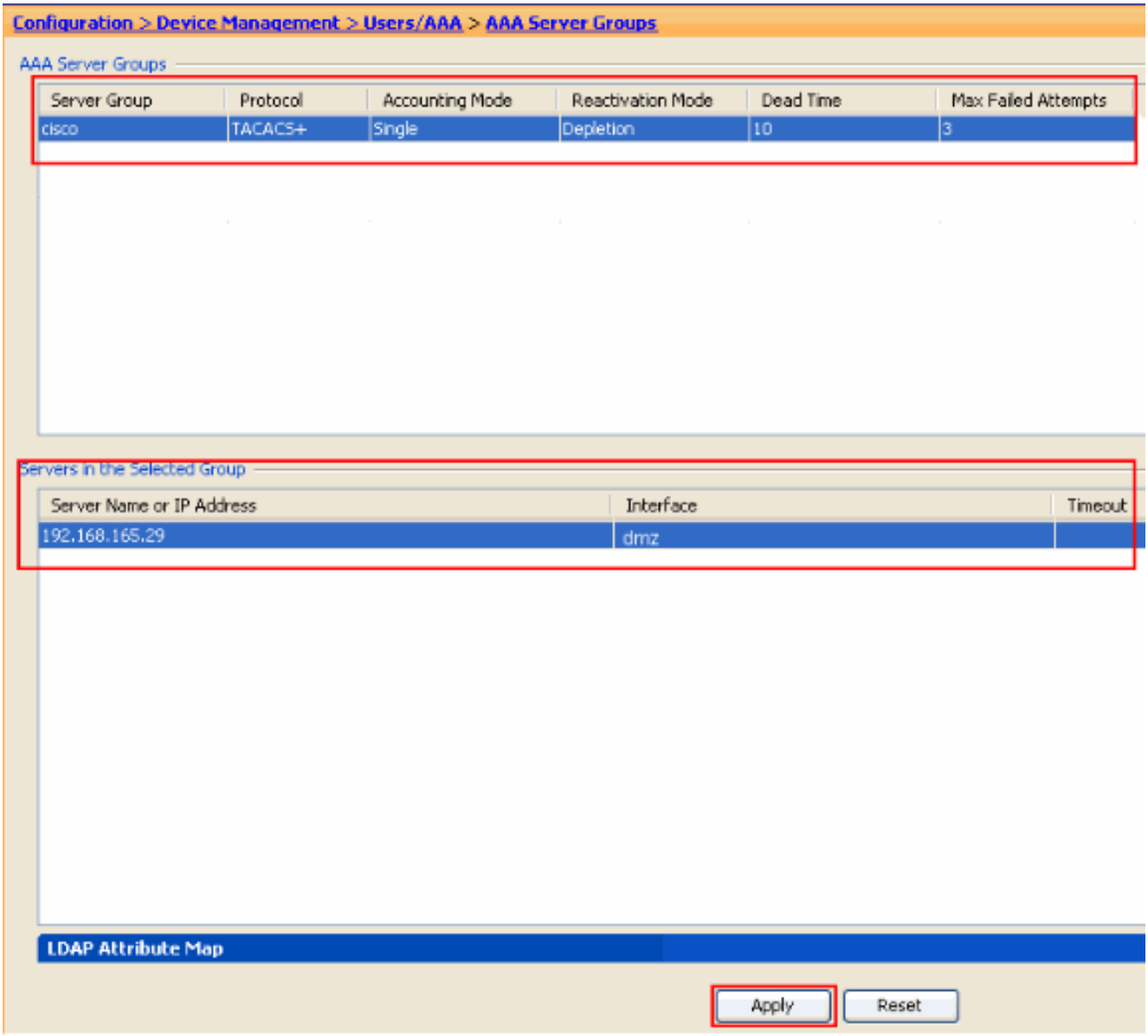
4. 표시된 대로 **AAA 서버 추가** 창에서 **AAA 서버** 세부 정보를 제공합니다.사용된 서버 그룹은 **cisco**입니다



. OK(**확인**)를 클릭한 다음 Apply(적용)를 **클릭합니다**.ASA에 구성된 **AAA 서버 그룹** 및 **AAA 서버**가 표시됩니다.

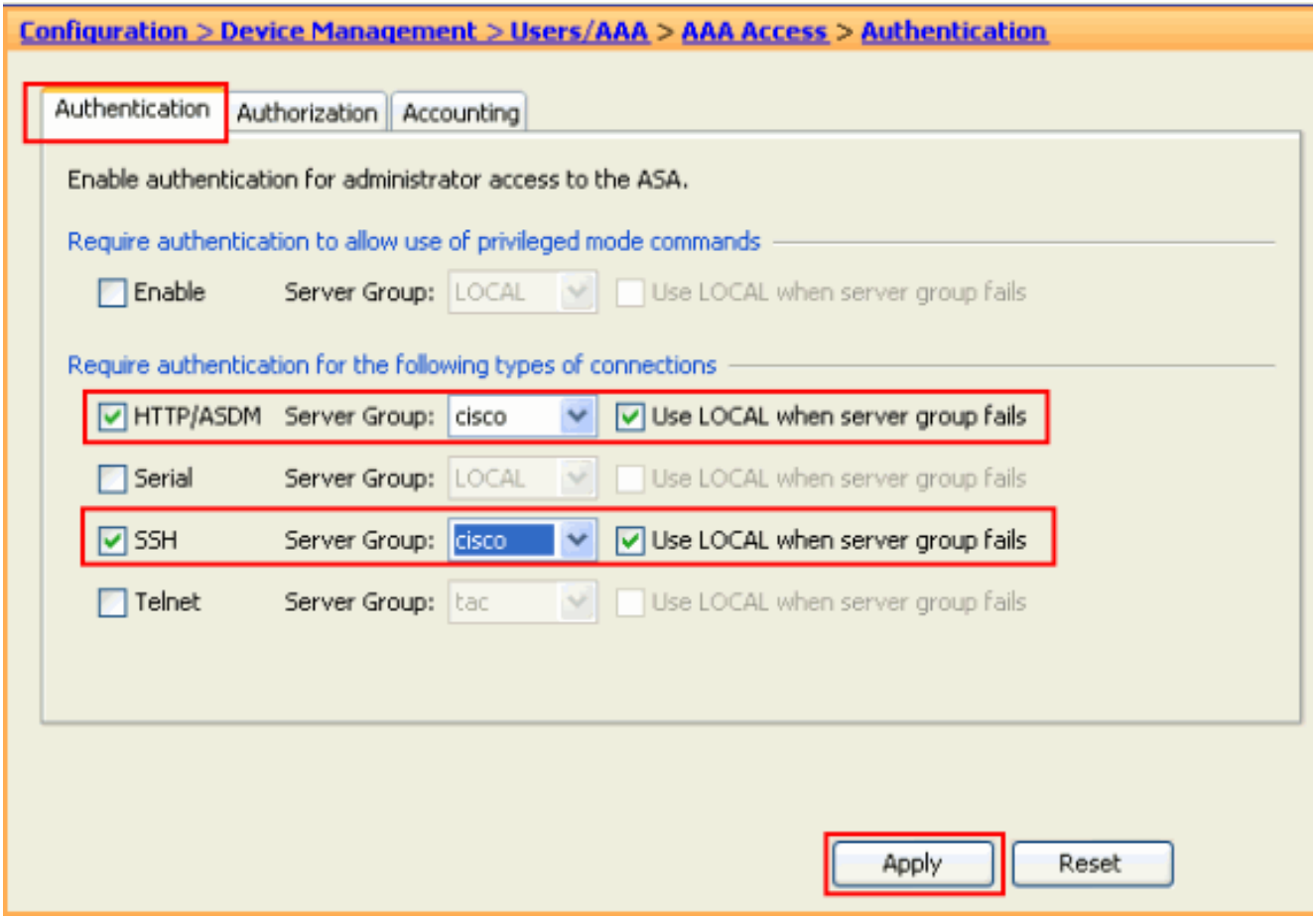
5. Apply를 **클릭합니다**

.



6. Configuration **> Device Management > Users/AAA > AAA Access > Authentication을 선택하고 HTTP/ASDM** 및 **SSH** 옆의 확인란을 **클릭합니다**.그런 다음 **cisco를** 서버 그룹으로 선택하고 Apply(적용)를 **클릭합니다**

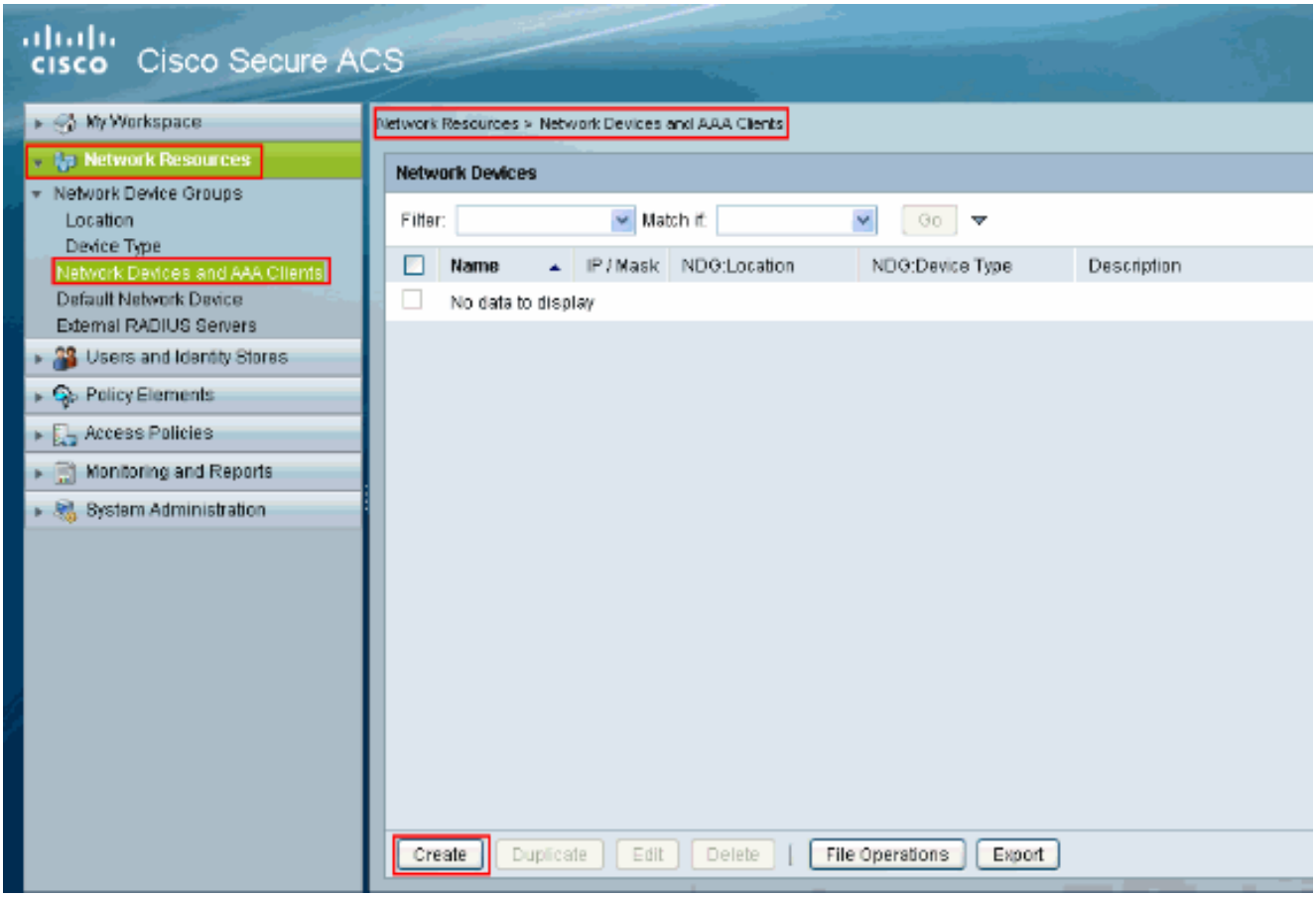
.



ACS를 TACACS 서버로 구성

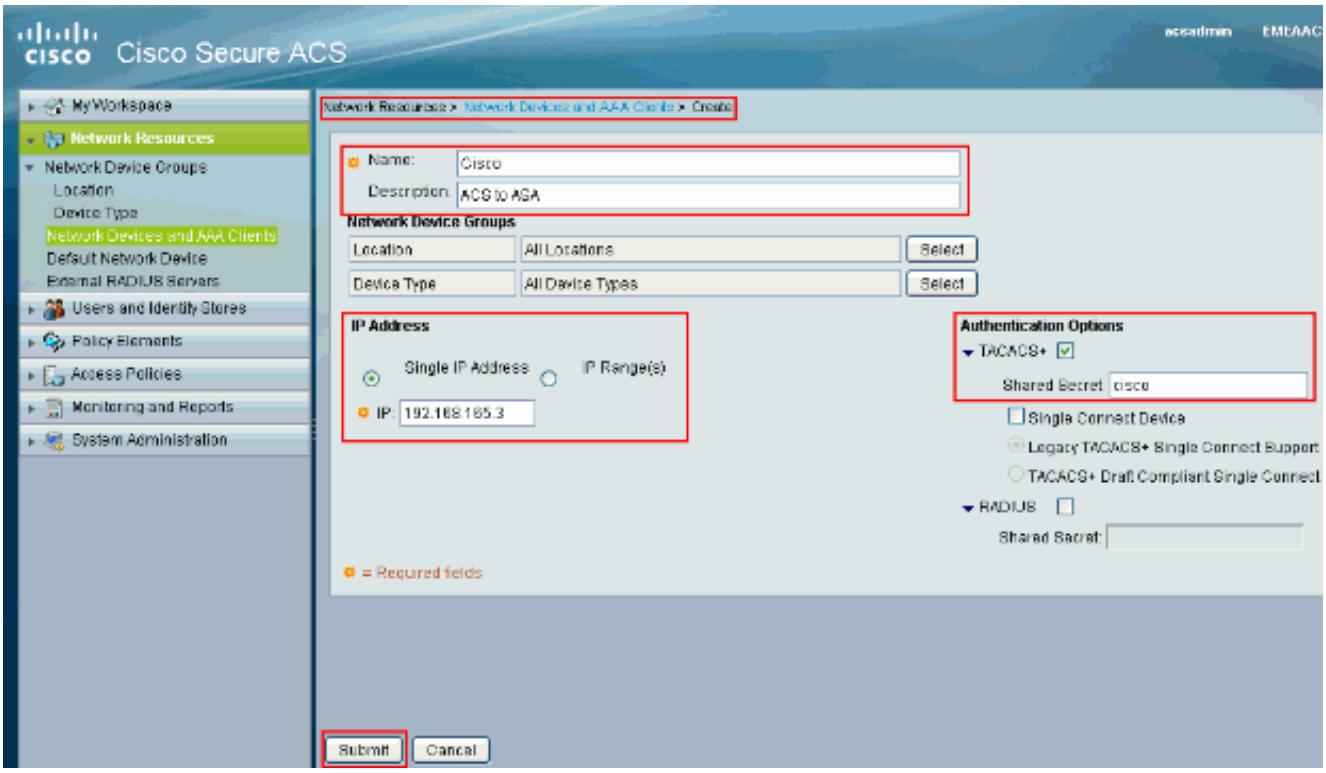
ACS를 TACACS 서버로 구성하려면 다음 절차를 완료합니다.

1. Network **Resources(네트워크 리소스) > Network Devices and AAA Clients(네트워크 디바이스 및 AAA 클라이언트)를** 선택하고 **Create**(생성)를 클릭하여 ACS 서버에 ASA를 추가합니다.



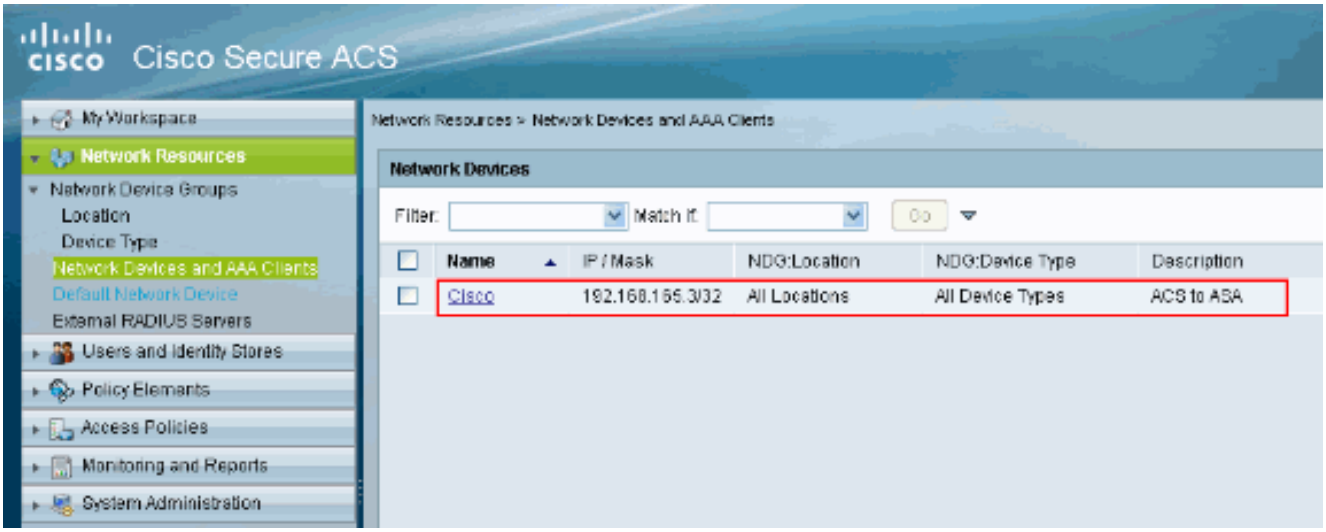
2. **클라이언트**에 대한 필수 정보를 제공하고 Submit(제출)을 **클릭합니다**.이렇게 하면 ASA가 ACS 서버에 추가될 수 있습니다.세부 정보에는 ASA의 **IP 주소**와 TACACS **서버** 세부사항이 포함됩니다

.



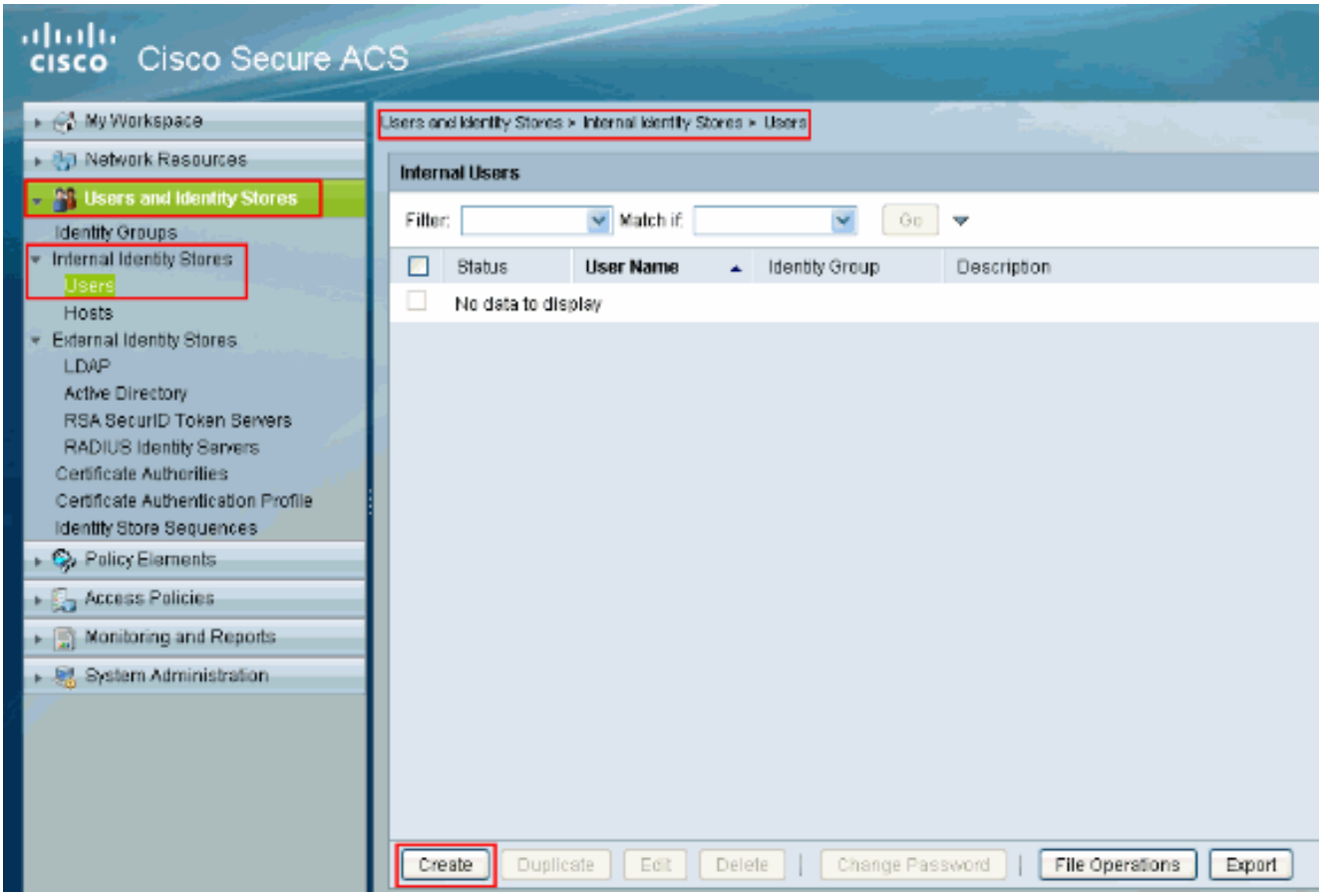
클라이언트 **Cisco**가 ACS 서버에 추가되고 있는 것을 볼 수 있습니다

.



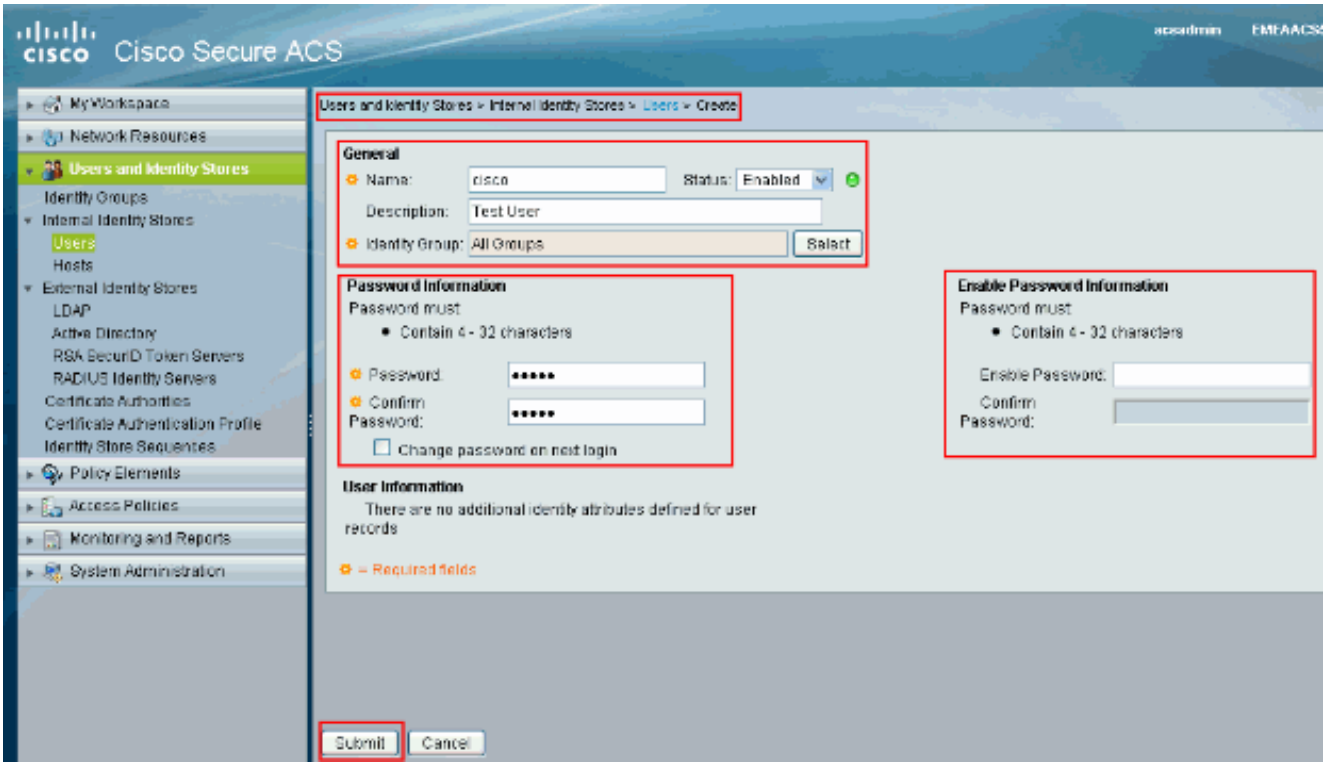
3. Users **and Identity stores(사용자 및 ID 저장소) > Internal Identity Stores(내부 ID 저장소) > Users(사용자)를** 선택하고 **Create(생성)를** 클릭하여 새 사용자를 생성합니다

.



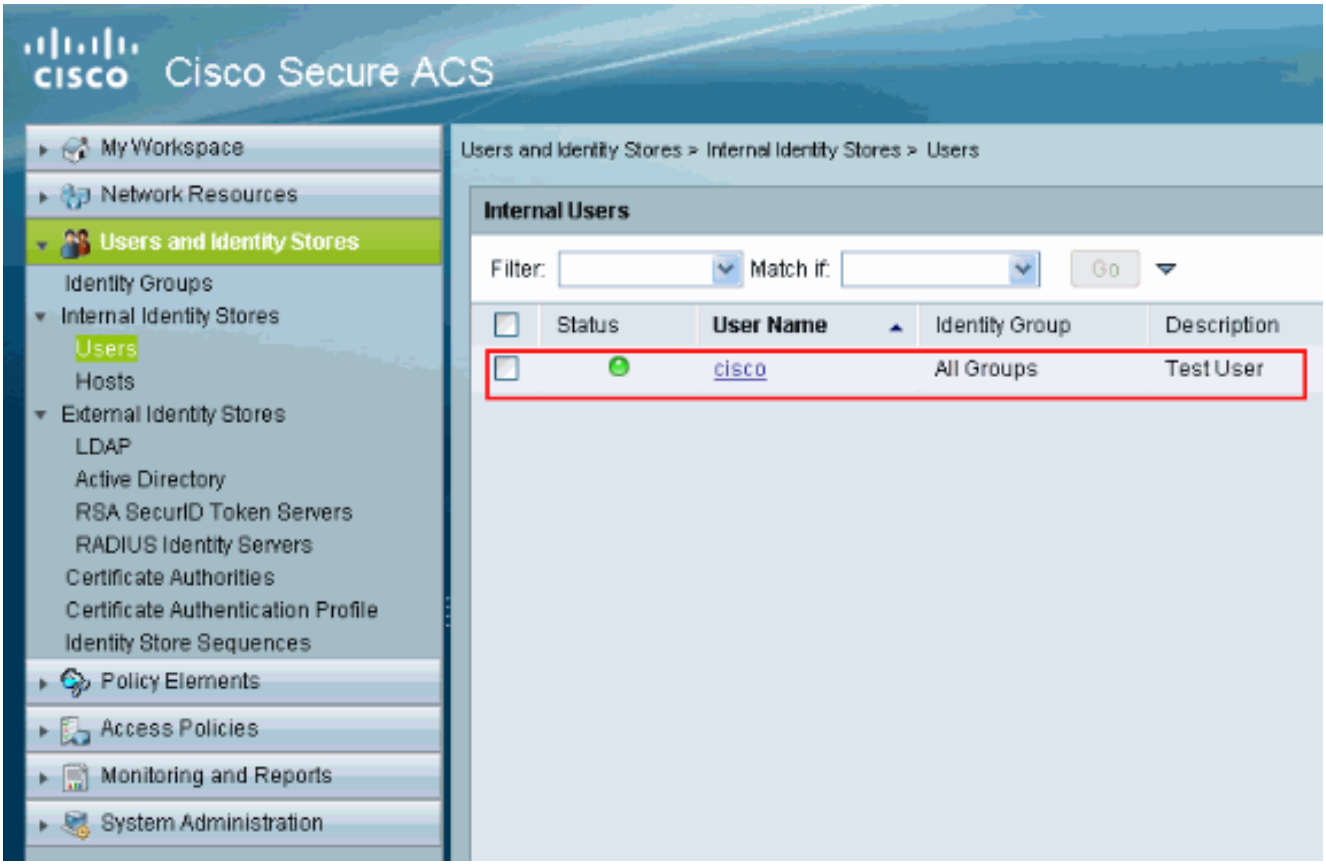
4. **이름, 비밀번호 및 비밀번호 활성화** 정보**를** 제공합니다.**Enable Password(비밀번호 활성화)**는 **선택 사항입니다**.완료되면 Submit(제출)을 **클릭합니다**

.



사용자 **cisco**가 ACS 서버에 추가되고 있습니다

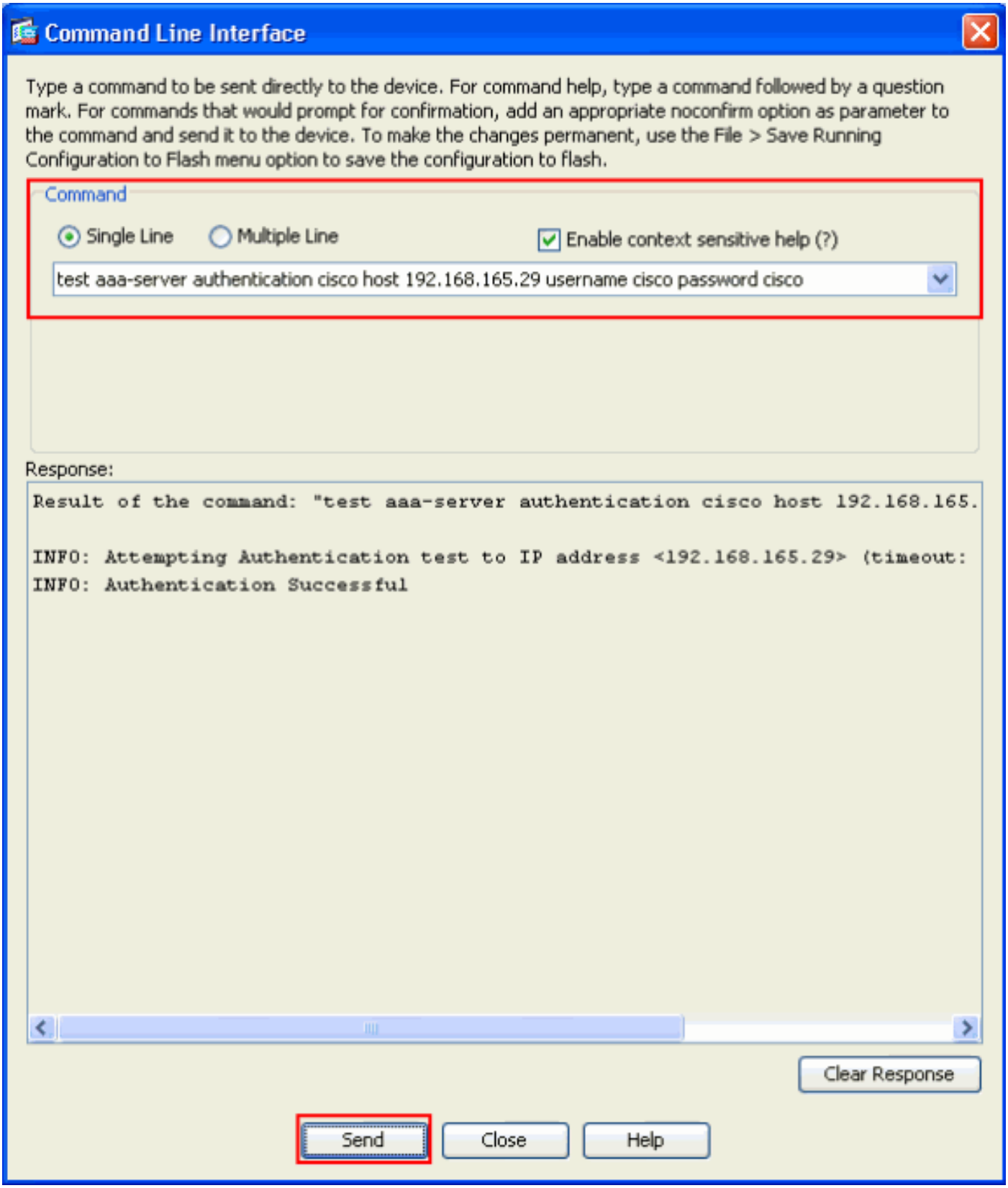
.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

가장 빠른 aaa-server authentication cisco host 192.168.165.29 username cisco password cisco 명령을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.이 그림에서는 인증이 성공했으며 ASA에 연결하는 사용자가 ACS 서버에서 인증되었음을 보여줍니다.



Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

문제 해결

오류:aaa-server group tacacs에서 TACACS+ 서버 x.x.x.x를 FAILED로 표시하는 AAA

이 메시지는 Cisco ASA가 x.x.x.x 서버와의 연결을 끊었음을 의미합니다.ASA에서 서버 x.x.x.x에 대한 tcp 49에서 유효한 연결이 있는지 확인합니다.네트워크 레이턴시가 발생하는 경우 TACACS+ 서버에 대한 ASA의 시간 제한을 5초에서 원하는 시간(초)으로 늘릴 수도 있습니다.ASA는 FAILED 서버 x.x.x.x에 인증 요청을 보내지 않습니다.그러나 aaa-server group tacacs에서 다음 서버를 사용합니다.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliances 지원 페이지
- Cisco ASA 5500 Series Adaptive Security Appliances 명령 참조
- Cisco Adaptive Security Device Manager
- IPsec 협상/IKE 프로토콜 지원 페이지
- Windows용 Cisco Secure Access Control Server
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems