ASA 8.3: TACACS-verificatie met behulp van ACS 5.X

Inhoud

Inleiding

Dit document bevat informatie over de manier waarop u het security apparaat kunt configureren om gebruikers te controleren op een netwerktoegang.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat de adaptieve security applicatie (ASA) volledig gebruiksklaar is en geconfigureerd om Cisco adaptieve security applicatie Manager (ASDM) of CLI in staat te stellen configuratie veranderingen door te voeren.

Opmerking: Raadpleeg HTTPS Access voor ASDM voor meer informatie over hoe u het apparaat op afstand kunt configureren door de ASDM.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Software voor Cisco adaptieve security applicatie, versie 8.3 en hoger
- Cisco adaptieve security applicatie Manager versie 6.3 en hoger

- Cisco Secure Access Control Server 5.x

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

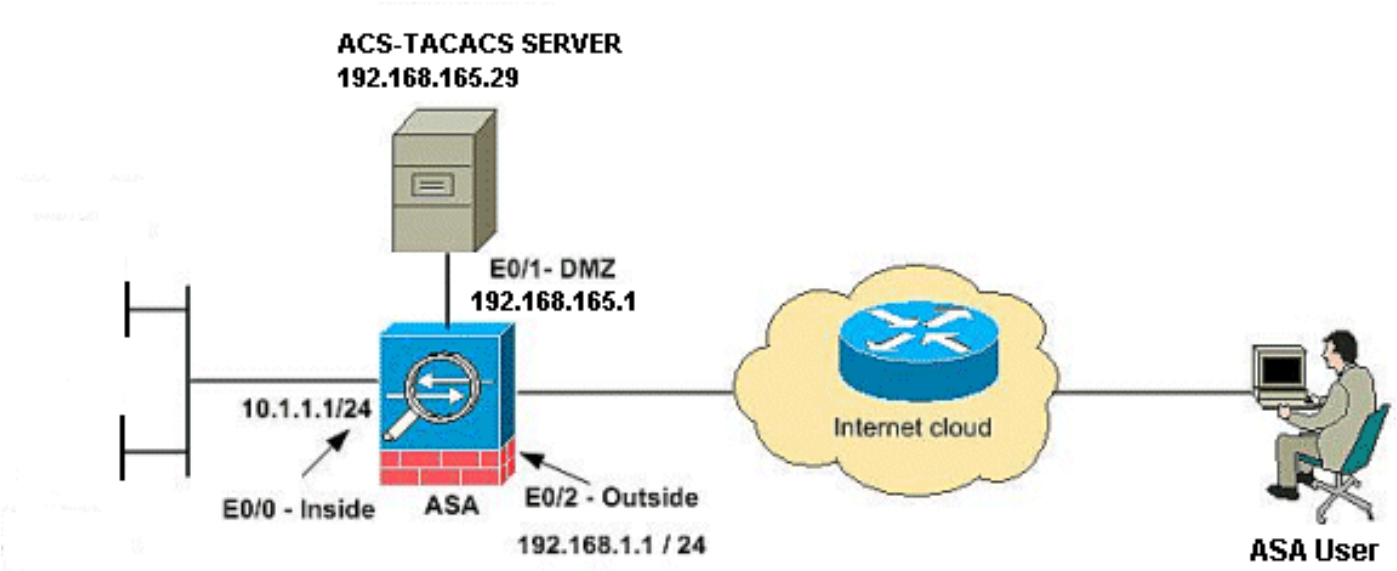
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Het zijn RFC 1918-adressen die in een labomgeving werden gebruikt.

Configureer de ASA voor verificatie vanaf de ACS-server met CLI

Voert deze configuraties voor de ASA uit om van de ACS server te authentiseren:

```
!--- 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
```

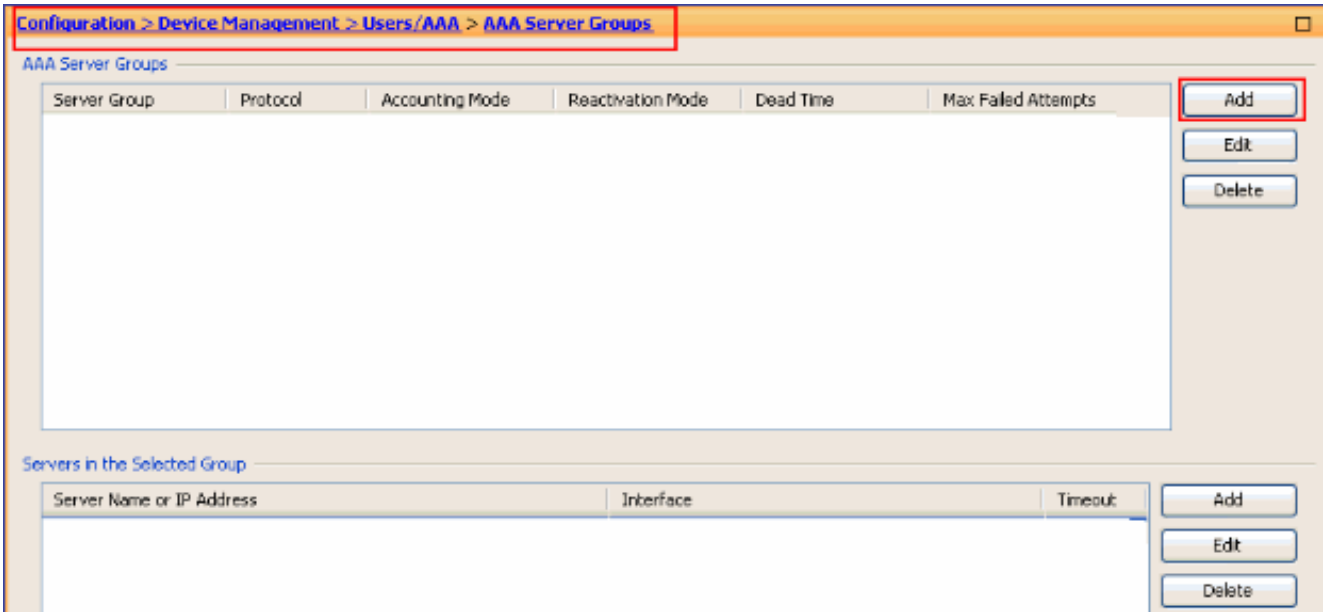
Opmerking: Maak een lokale gebruiker op de ASA met de **gebruikersnaam cisco password cisco bevoorrecht 15 opdracht om** ASDM met lokale authenticatie te benaderen wanneer ACS niet beschikbaar is.

ASA configureren voor verificatie vanaf ACS-server met ASDM

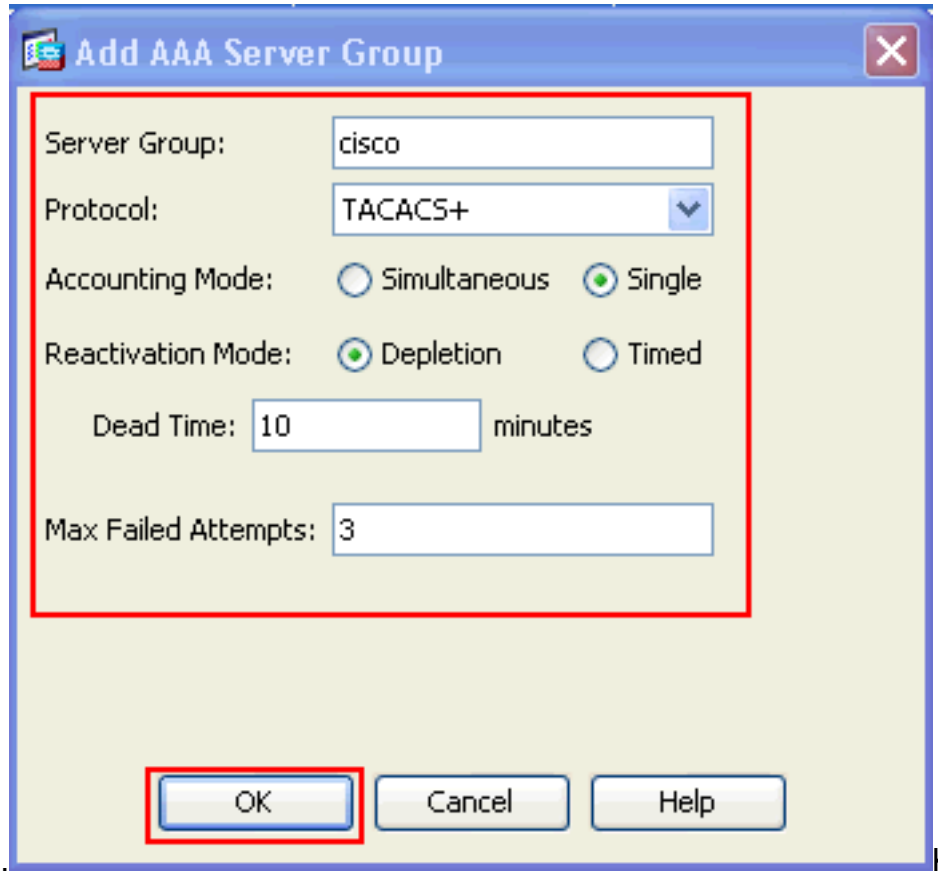
ASDM-procedure

Voltooi deze stappen om de ASA voor verificatie van de ACS-server te configureren:

1. Kies **Configuratie > Apparaatbeheer > Gebruikers/AAA > AAA-servergroepen > Toevoegen** om een **AAA-servergroep** te maken.

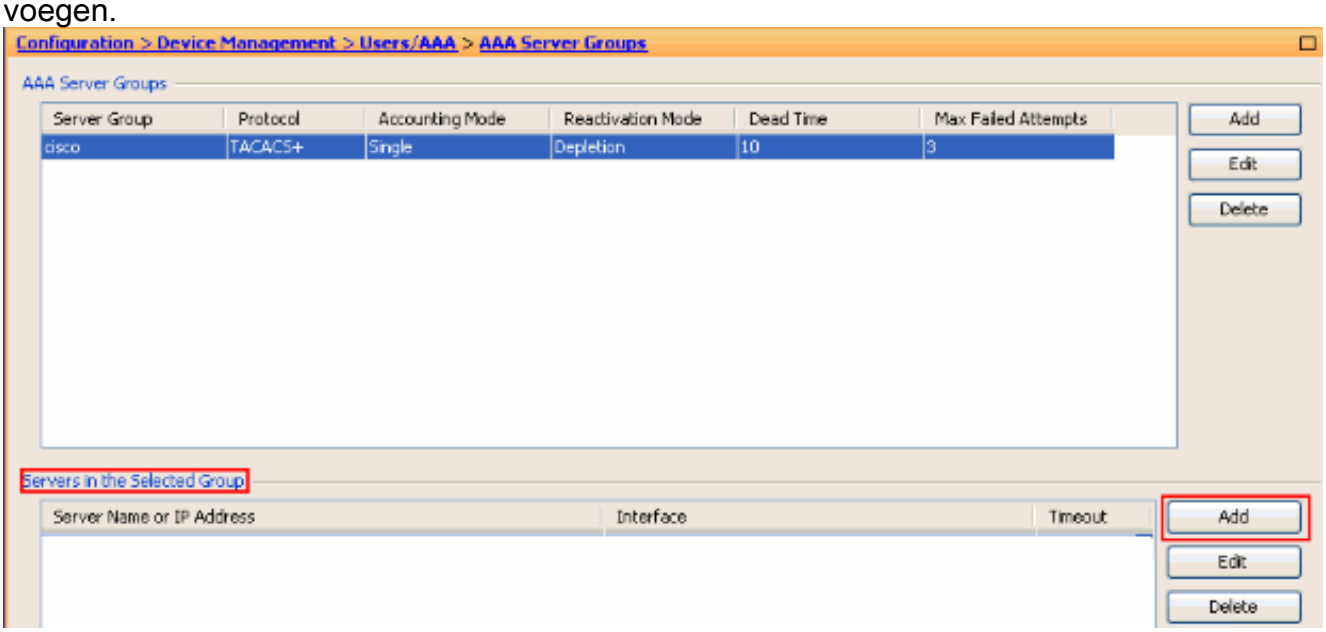


2. Geef de gegevens van de **AAA-servergroep op** in het venster **AAA-servergroep** toevoegen zoals weergegeven. Het gebruikte protocol is **TACACS+** en de servergroep die is gemaakt,

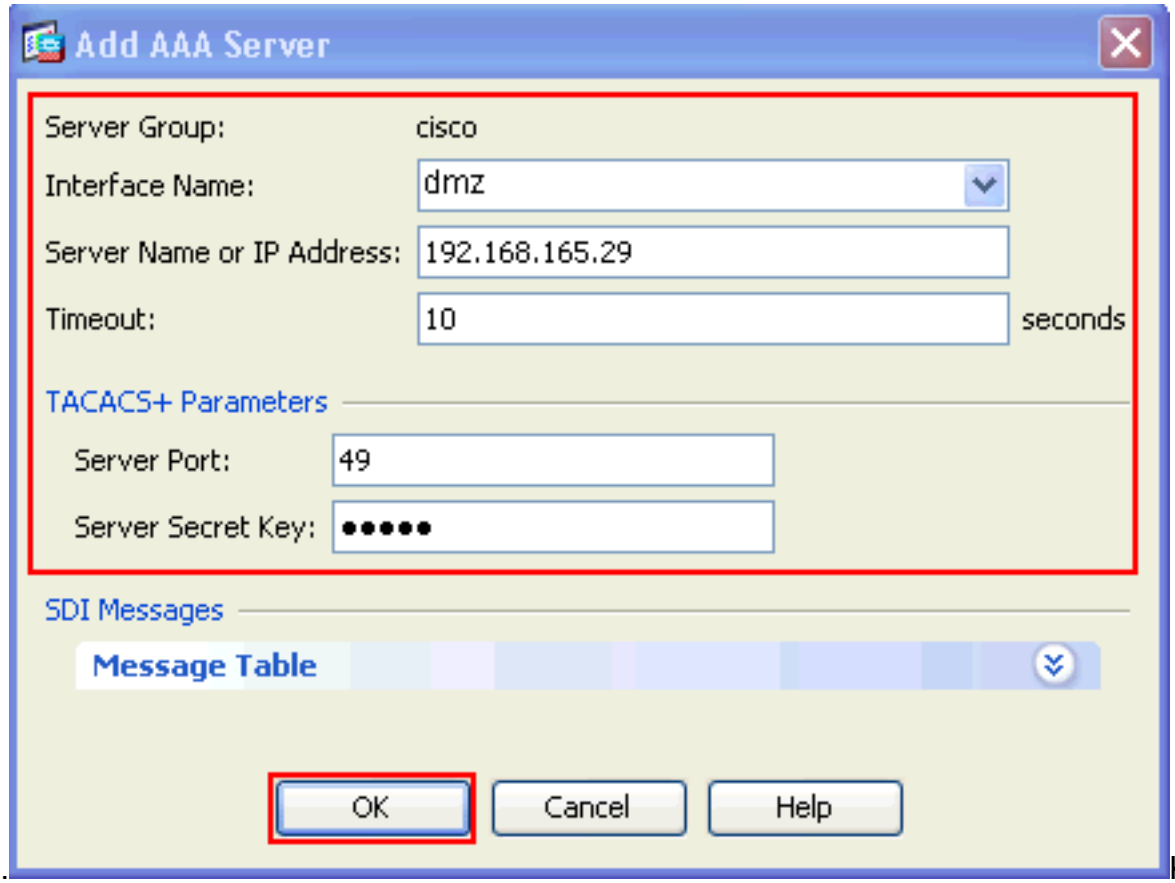


is **cisco**. Klik op **OK**.

3. Kies **Configuration > Apparaatbeheer > Gebruikers/AAA > AAA-servergroepen** en klik op **Add** onder **Server in de Geselecteerde groep** om de AAA-server toe te voegen.

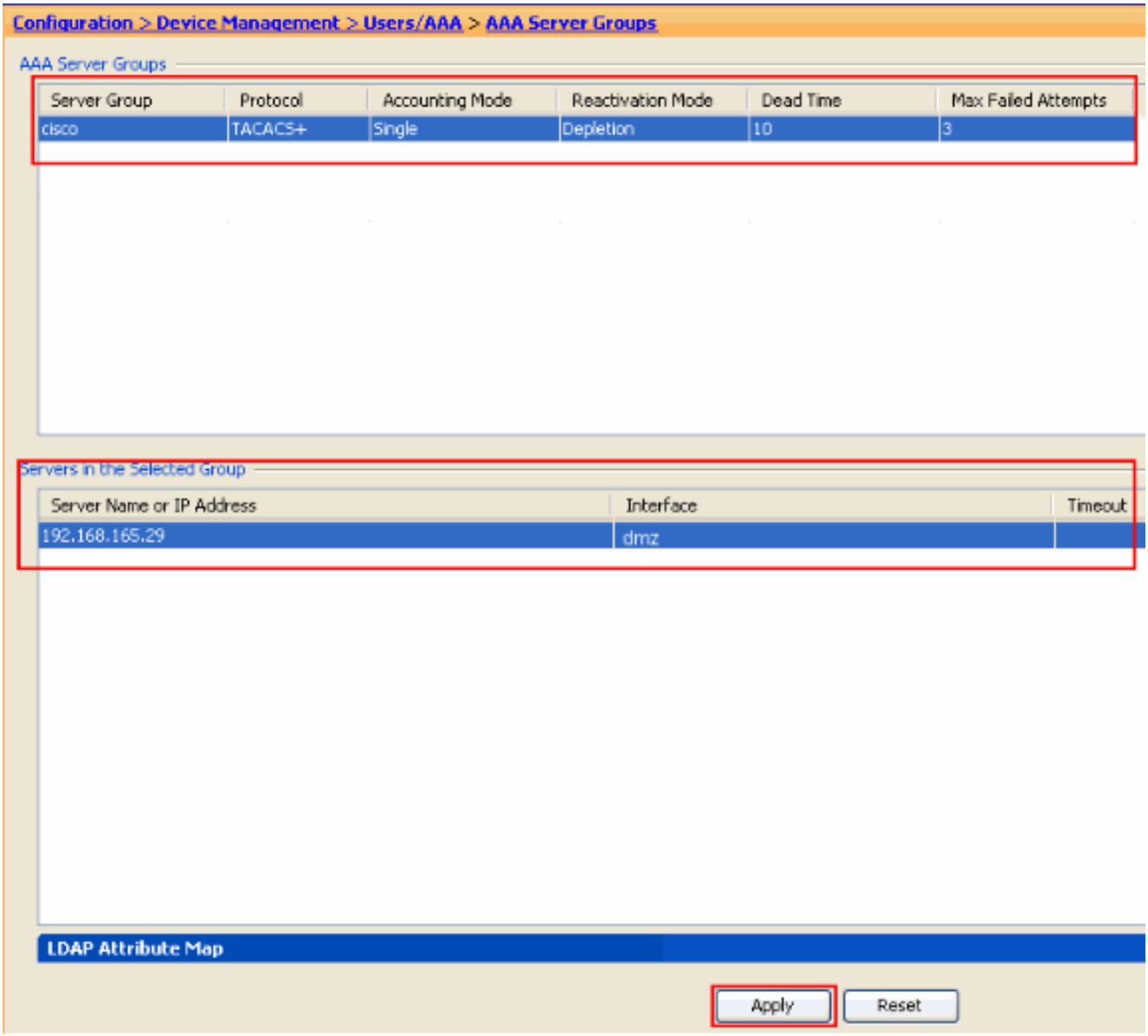


4. Geef de informatie over de **AAA-server op** in het venster **Add AAA Server** zoals weergegeven. De gebruikte servergroep is

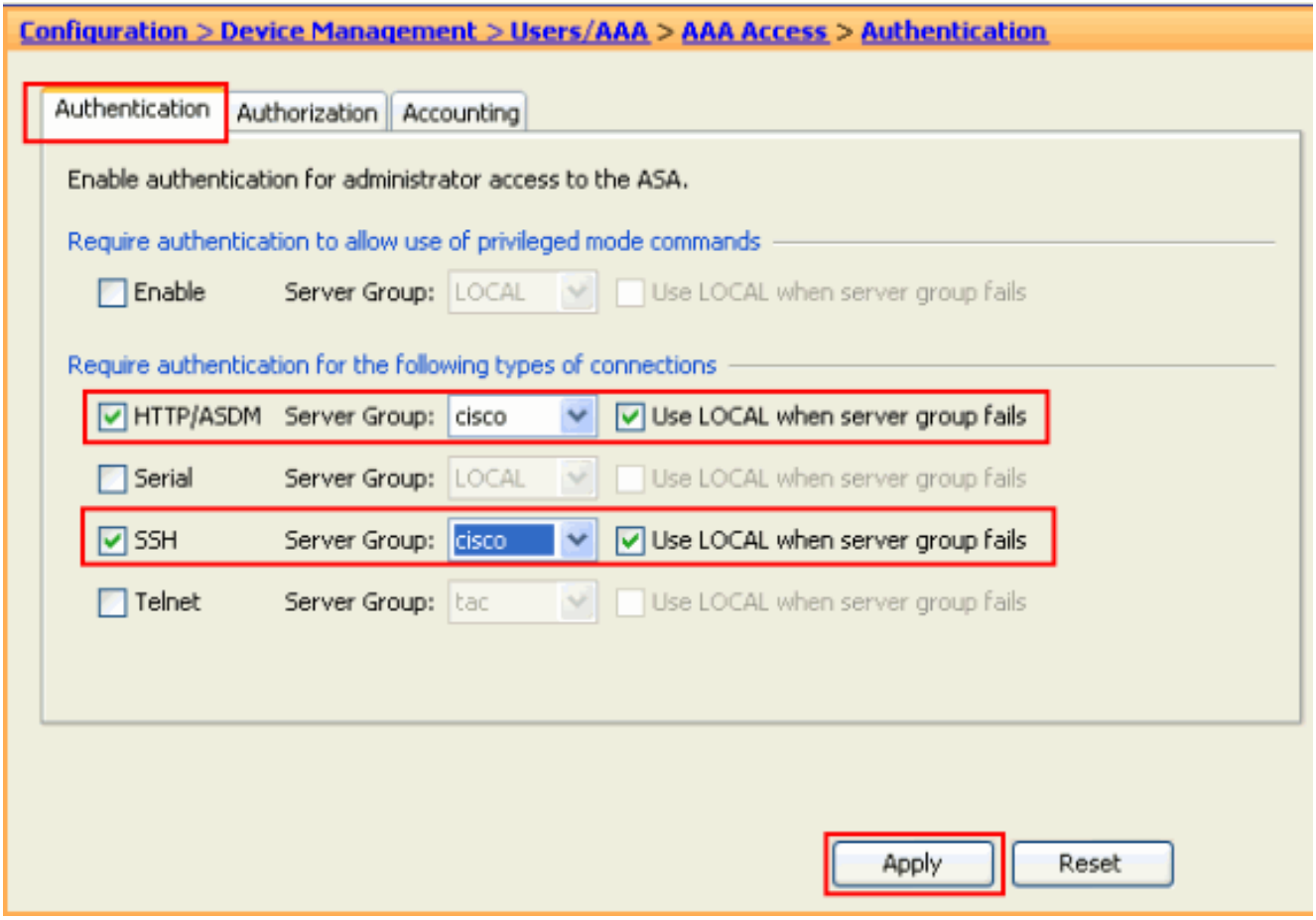


cisco.Klik op **OK** en vervolgens op **Toepassen**.U ziet de **AAA-servergroep** en de **AAA-server** die in de ASA zijn geconfigureerd.

5. Klik op **Toepassen**.



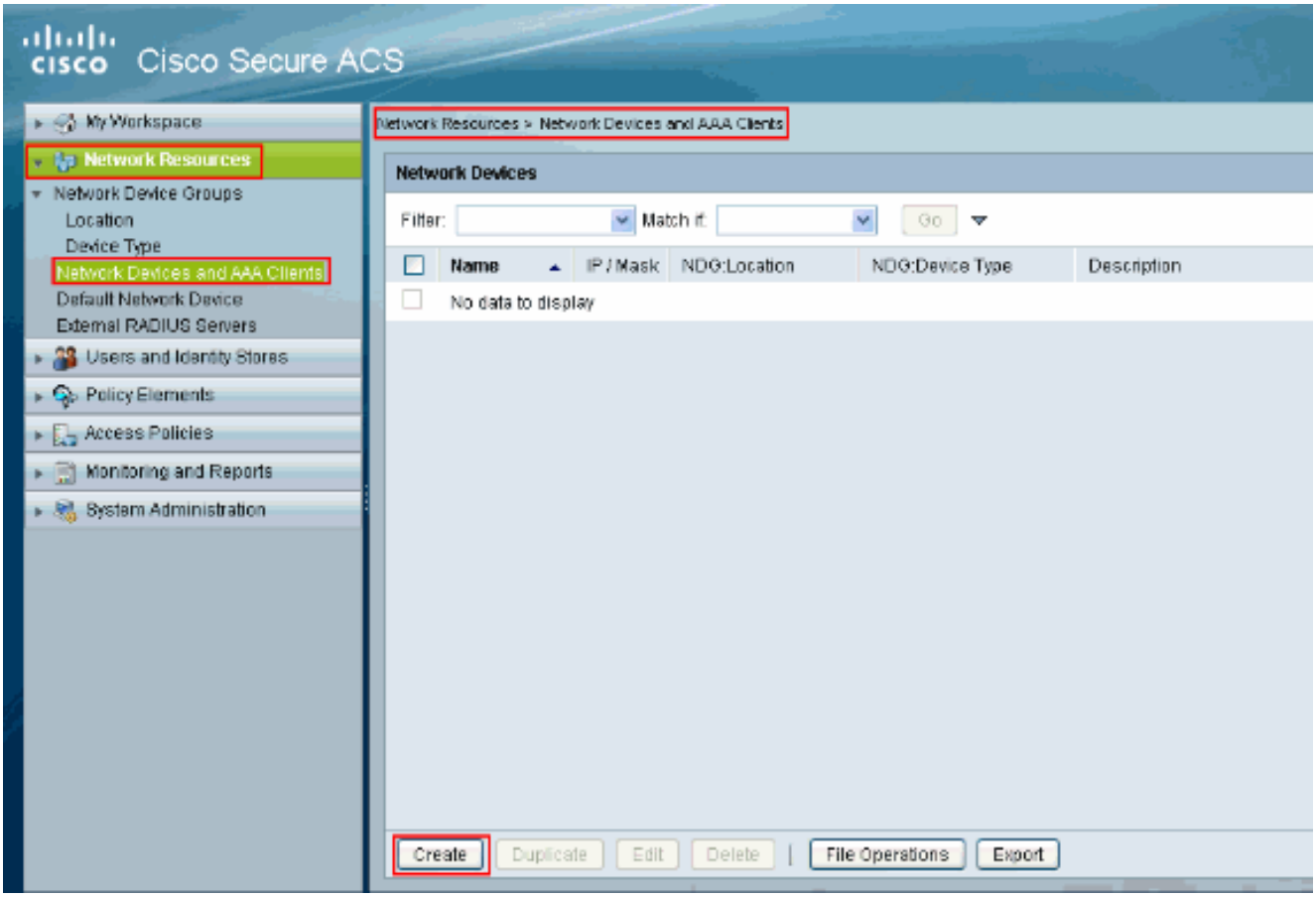
6. Kies **Configuratie > Apparaatbeheer > Gebruikers/AAA > Toegang > Verificatie** en klik op de vinkjes naast **HTTP/ASDM** en **SSH**. Kies vervolgens **cisco** als de servergroep en klik op **Toepassen**.



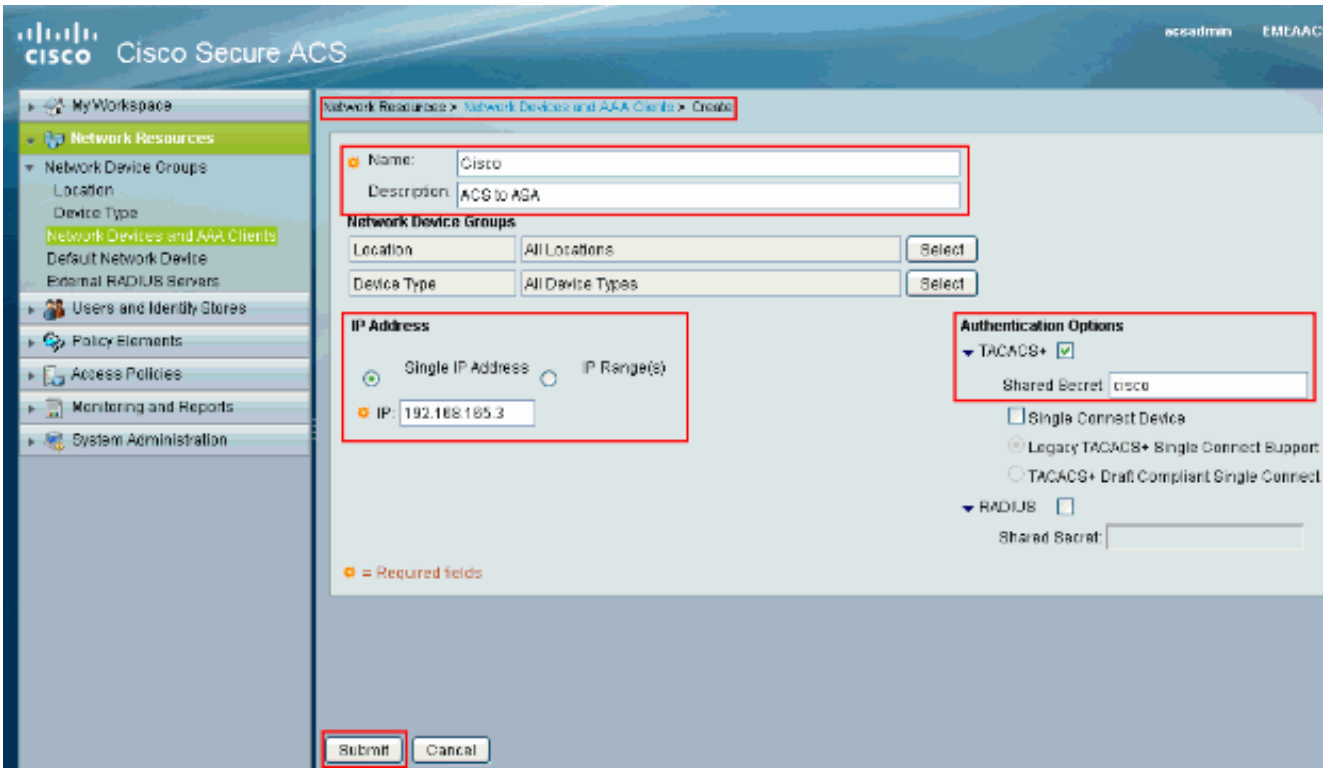
ACS als een TACACS-server configureren

Voltooi deze procedure om ACS als een TACACS-server te configureren:

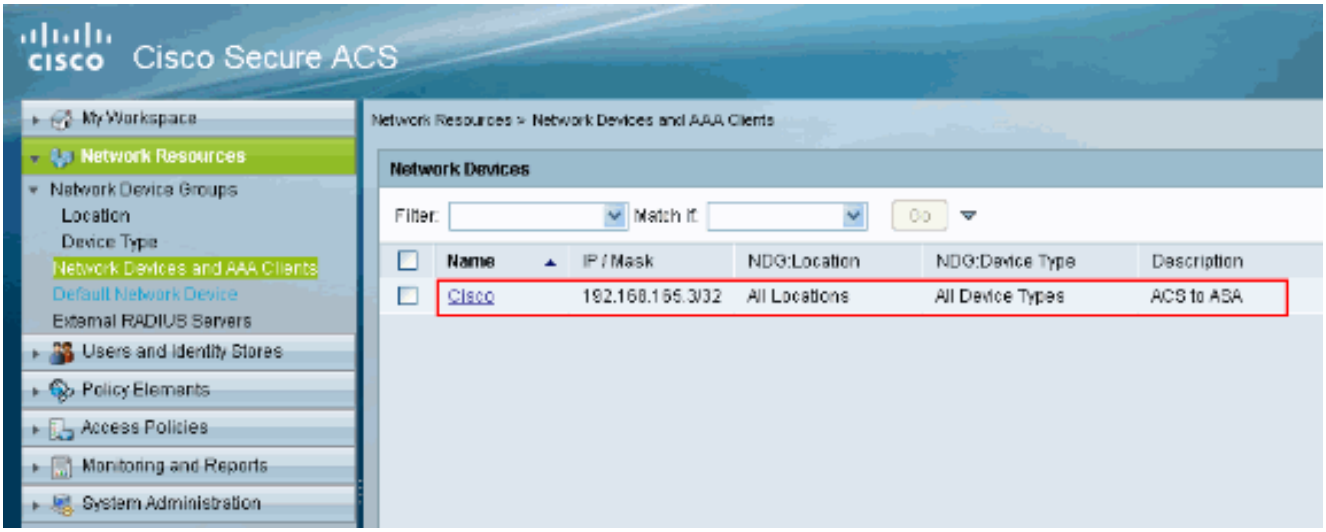
1. Kies **Netwerkbronnen > Netwerkapparaten en AAA-clients** en klik op **Maken** om de ASA aan de ACS-server toe te
voegen.



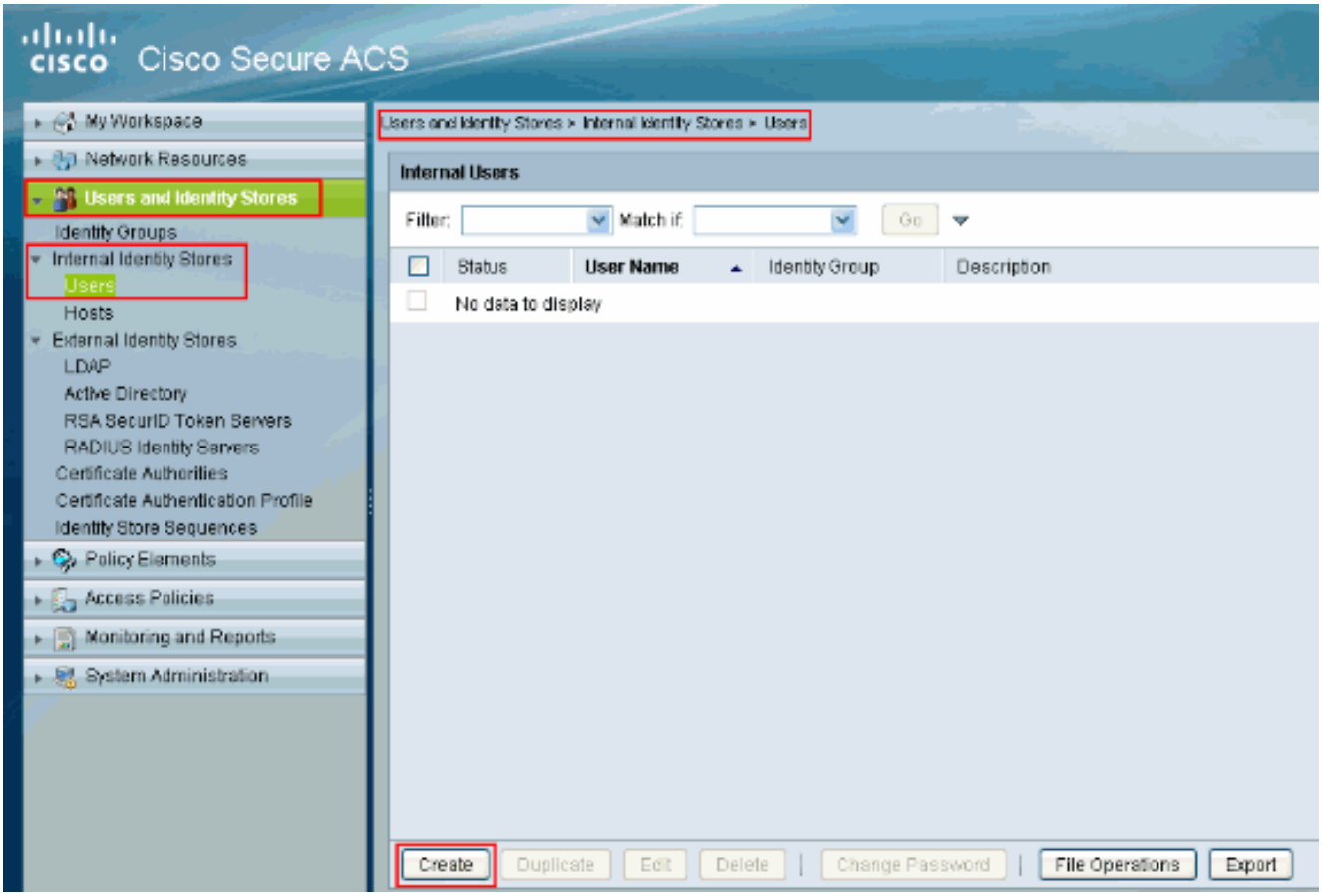
2. Verstrek de vereiste informatie over de **client** (ASA is hier de client) en klik op **Inzenden**. Hierdoor kan de ASA worden toegevoegd aan de ACS-server. De details omvatten het **IP-adres** van de ASA en de **TACACS server** details.



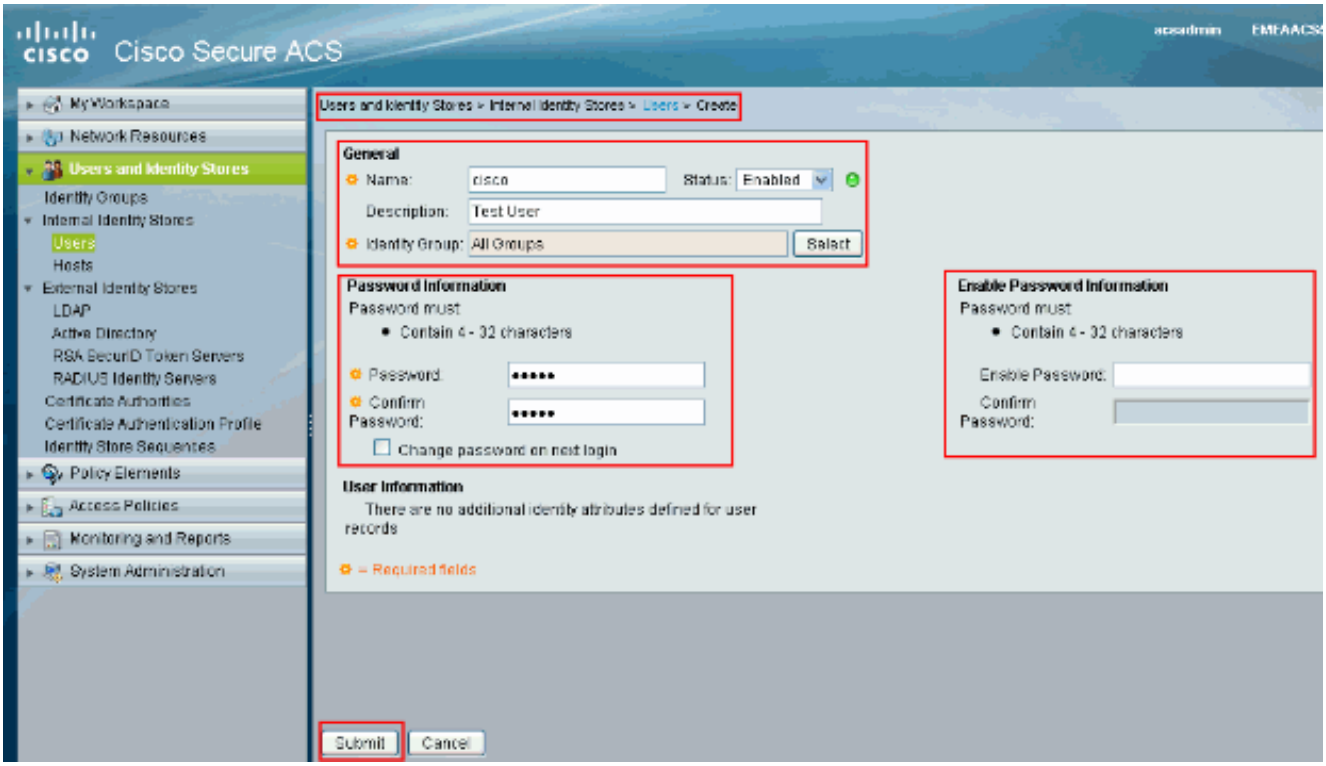
U ziet dat de client-**Cisco** wordt toegevoegd aan de ACS-server.



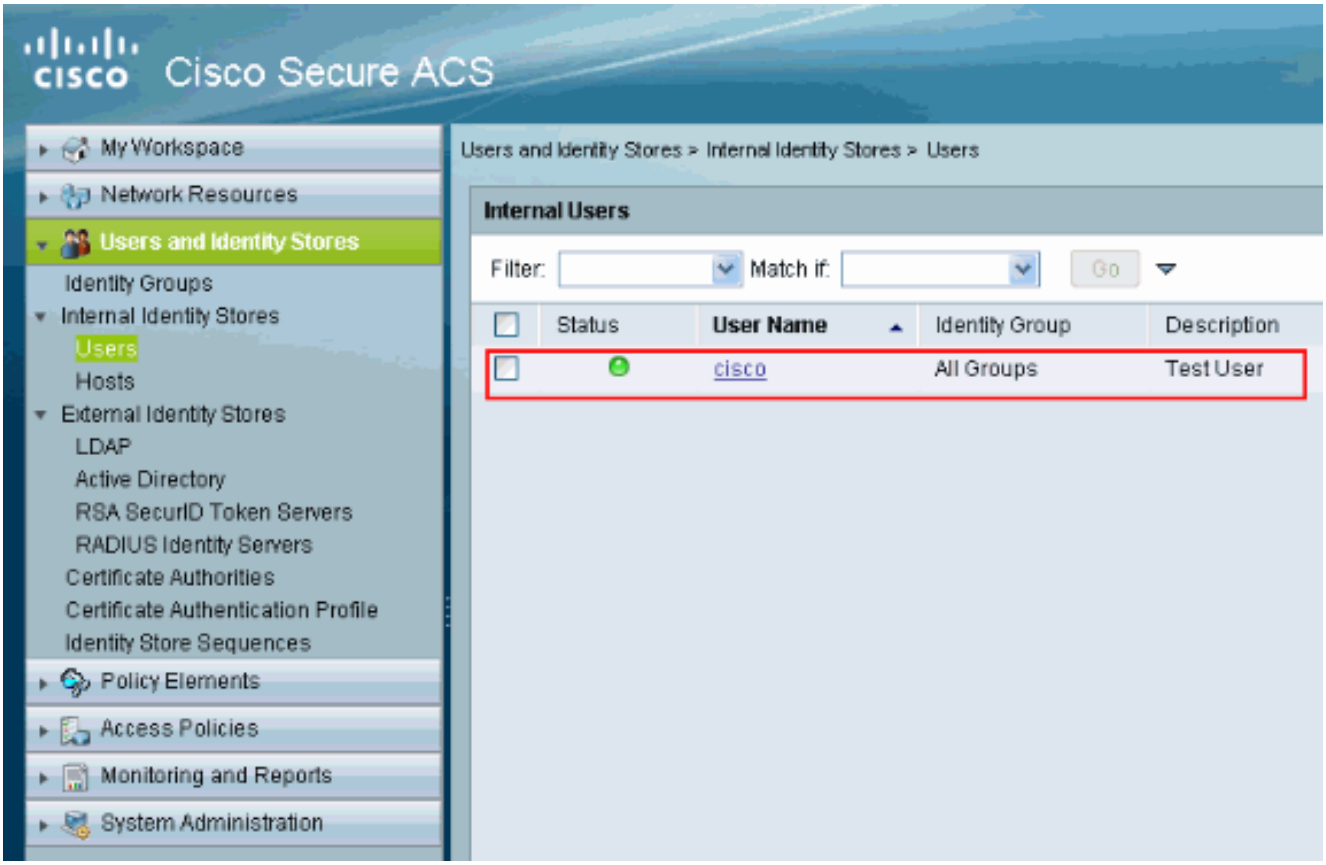
3. Kies **gebruikers en identiteitsopnamen > Interne identiteitsopslag > Gebruikers** en klik op **Maken** om een nieuwe gebruiker te maken.



4. Typ de informatie **Naam, Wachtwoord en Wachtwoord inschakelen**. **Wachtwoord inschakelen** is **optioneel**. Klik op **Inzenden** als u klaar bent.



U ziet dat de gebruiker **cisco** wordt toegevoegd aan de ACS-server.

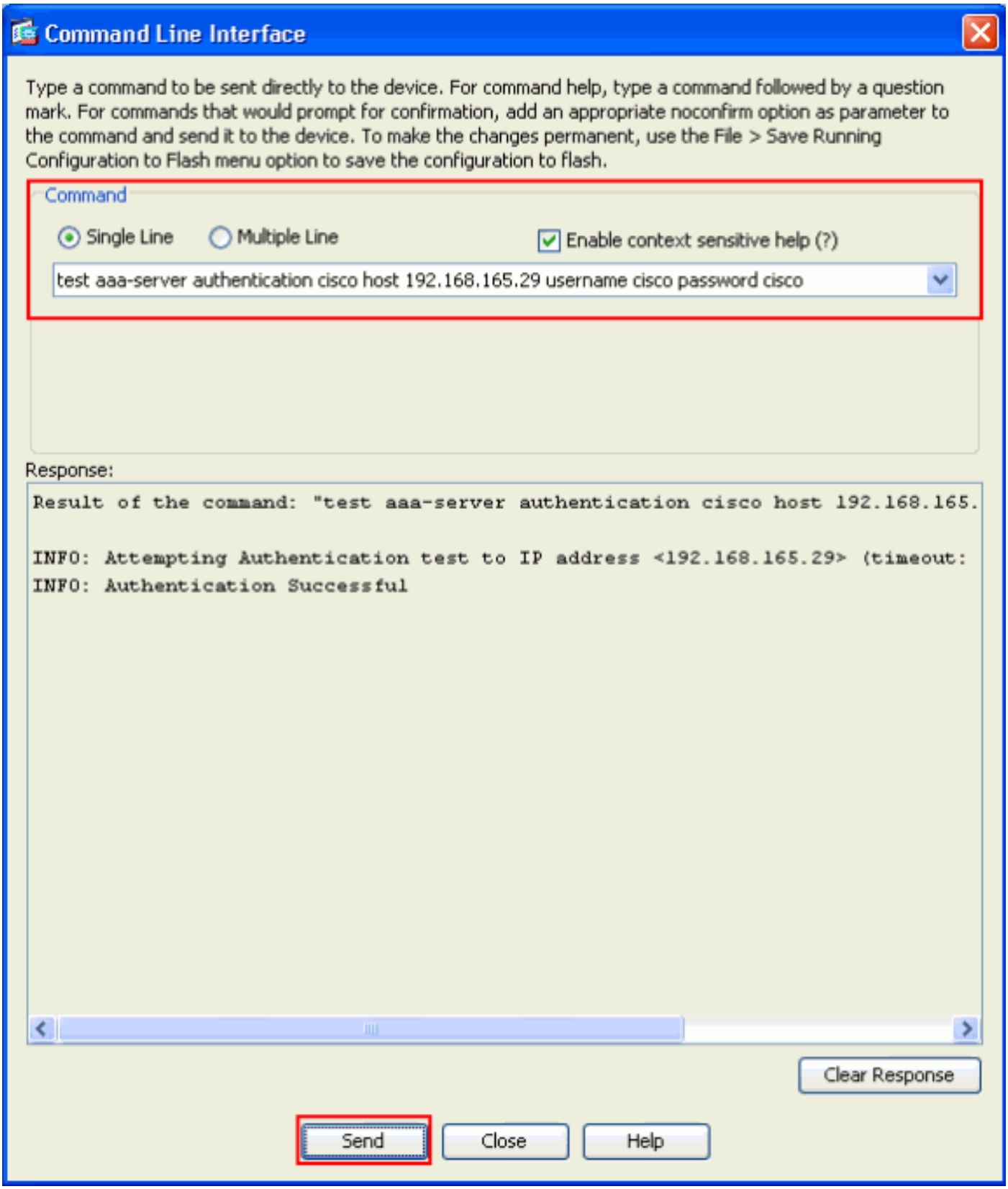


Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Gebruik **de** opdracht **cisco** van de **gebruikersnaam voor Cisco voor de** configuratie **van de** Cisco-**server** op **de** testbasis **cisco host 192.168.165.29** om te controleren of de configuratie correct werkt. Dit beeld toont aan dat de authenticatie succesvol is en de gebruiker die verbinding maakt

met de ASA is geauthentiseerd door de ACS server.



Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Problemen oplossen

Fout: AAA-markering voor TACACS+ server x.x.x.x in tac's van de a-server als

FAILLE

Dit bericht betekent dat Cisco ASA de connectiviteit met de x.x.x.x server verloor. Zorg ervoor dat u een geldige verbinding op tcp 49 hebt om x.x.x van de ASA server te serveren. U kunt de time-out op de ASA-server voor TACACS+ ook verhogen van 5 naar het gewenste aantal seconden voor het geval er een netwerkvertraging is. ASA zou geen verificatieaanvraag naar de FAILED server x.x.x.x sturen. Het gebruikt echter de volgende server in de tac's van de a-server groep.

Gerelateerde informatie

- Cisco ASA 5500 Series ondersteuningspagina voor adaptieve security applicaties
- Cisco ASA 5500 Series Opdrachten voor adaptieve security applicaties
- Cisco adaptieve security apparaatbeheer
- Ondersteuning van IPsec-onderhandeling/IKE-protocollen
- Cisco Secure Access Control Server voor Windows
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems