ASA 8.3: TACACS-Authentifizierung mit ACS 5.X

Inhalt

Einführung

Dieses Dokument enthält Informationen zur Konfiguration der Sicherheits-Appliance zur Authentifizierung von Benutzern für den Netzwerkzugriff.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass die Adaptive Security Appliance (ASA) voll funktionsfähig und so konfiguriert ist, dass der Cisco Adaptive Security Device Manager (ASDM) oder die CLI Konfigurationsänderungen vornehmen kann.

Hinweis: Weitere Informationen zur Remote-Konfiguration des Geräts durch den ASDM finden Sie unter Zulassen von HTTPS-Zugriff für ASDM.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliance Software Version 8.3 oder höher
- Cisco Adaptive Security Device Manager Version 6.3 und höher

- Cisco Secure Access Control Server 5.x

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

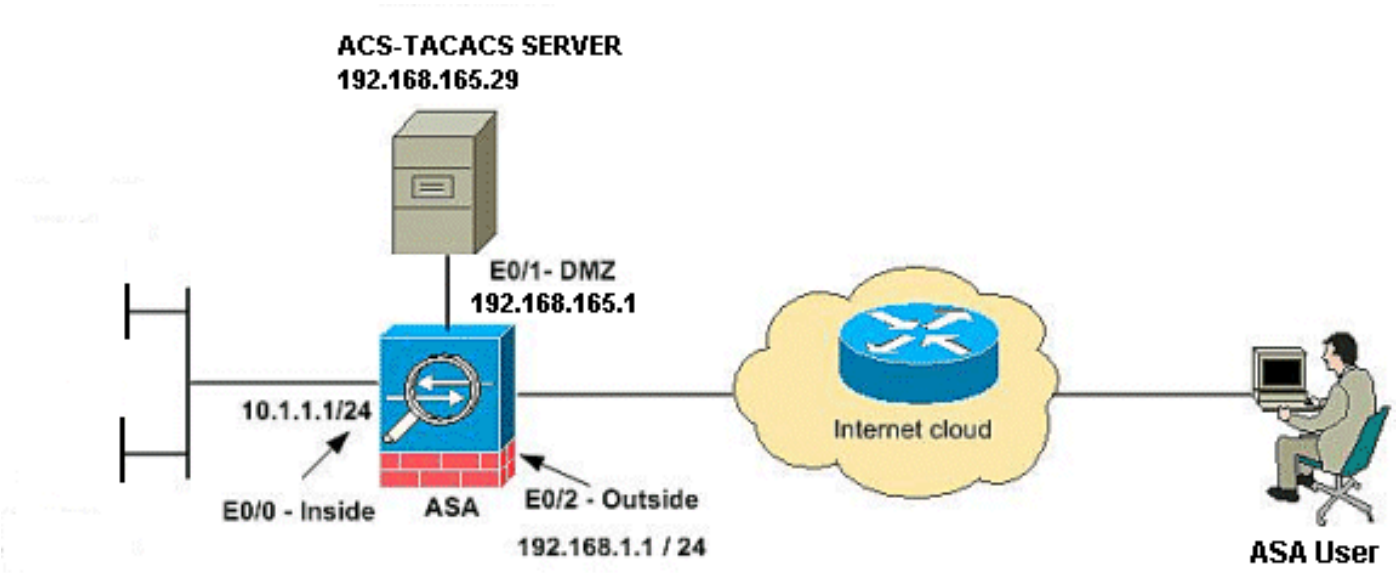
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Es handelt sich um RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

Konfigurieren der ASA für die Authentifizierung vom ACS-Server mithilfe der CLI

Führen Sie folgende Konfigurationen durch, damit die ASA vom ACS-Server authentifiziert werden kann:

```
!--- 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
```

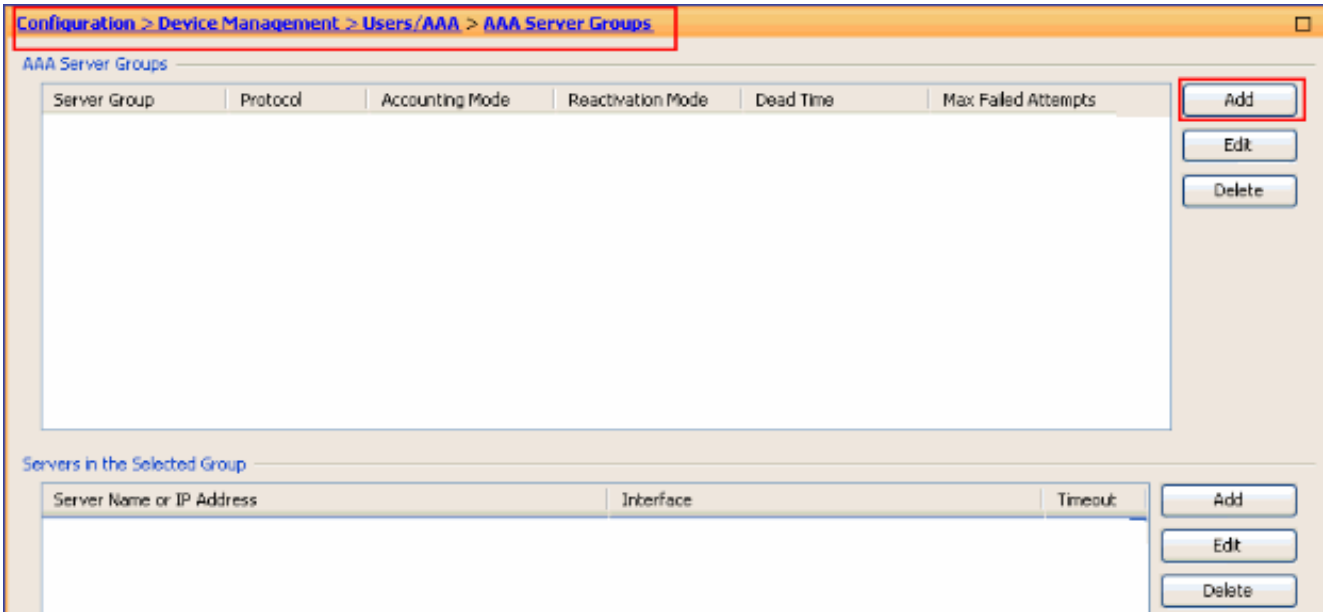
Hinweis: Erstellen Sie einen lokalen Benutzer auf der ASA mit dem **Befehl** username cisco password cisco privilege 15, um auf das ASDM mit lokaler Authentifizierung zuzugreifen, wenn der ACS nicht verfügbar ist.

Konfigurieren der ASA für die Authentifizierung vom ACS-Server mithilfe von ASDM

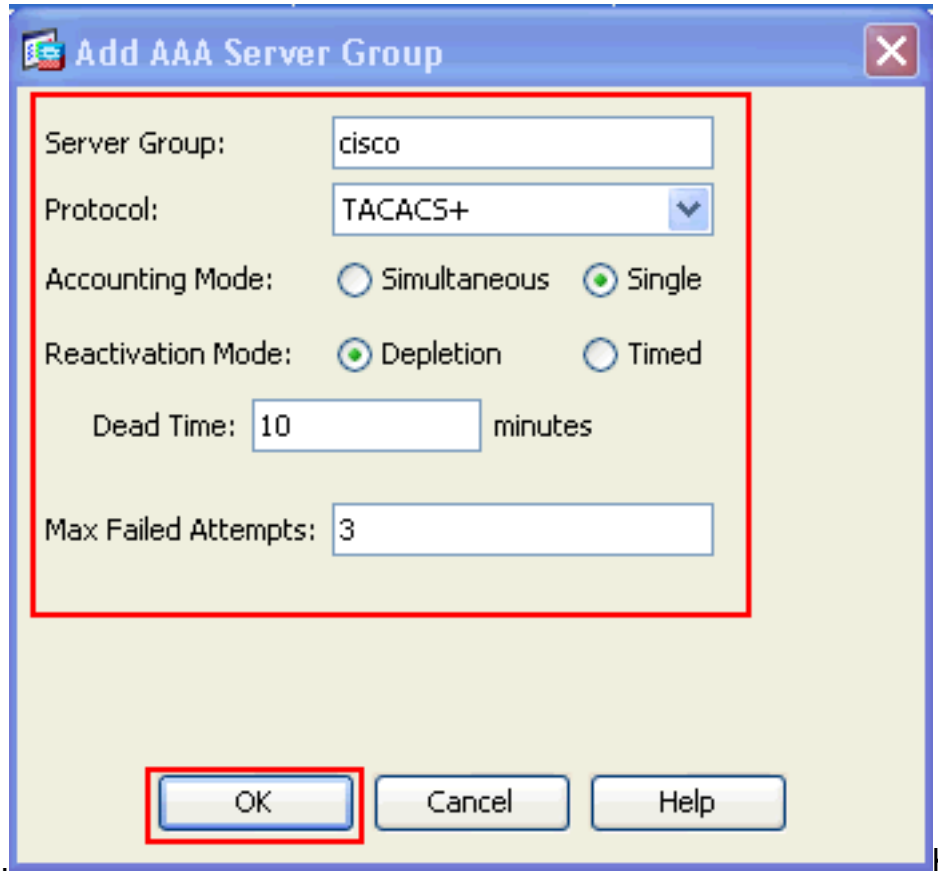
ASDM-Verfahren

Gehen Sie wie folgt vor, um die ASA für die Authentifizierung vom ACS-Server zu konfigurieren:

1. Wählen Sie **Configuration > Device Management > Users/AAA > AAA Server Groups > Add** aus, um eine **AAA-Servergruppe** zu erstellen.

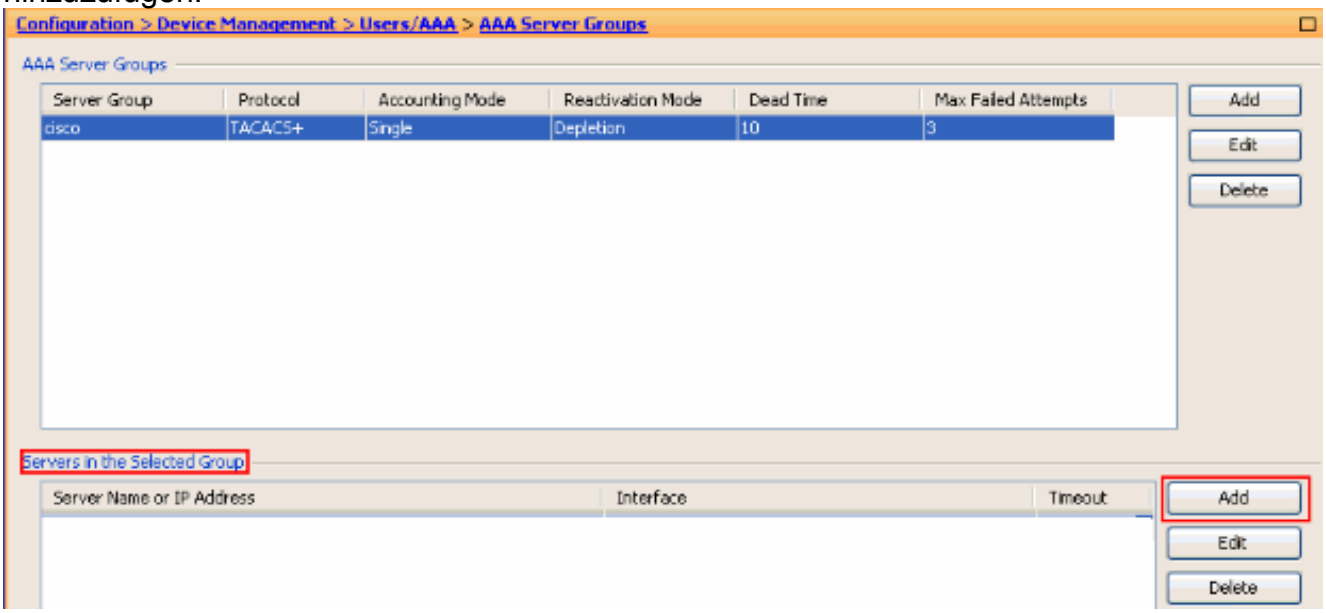


2. Geben Sie die **AAA-Servergruppen-**Details im Fenster **AAA-Servergruppe hinzufügen** wie gezeigt ein. Das verwendete Protokoll ist **TACACS+**, und die erstellte Servergruppe ist

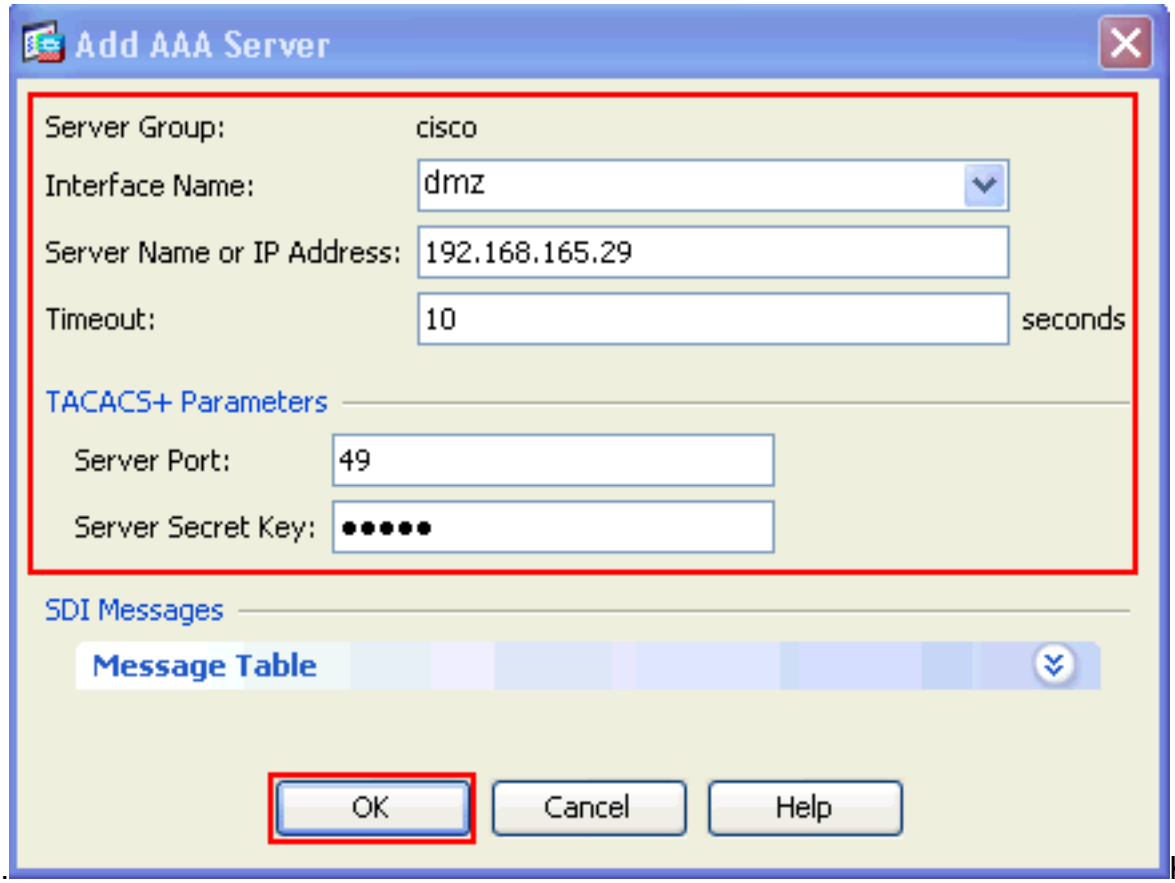


cisco. Klicken Sie auf **OK**.

3. Wählen Sie **Configuration > Device Management > Users/AAA > AAA Server Groups** aus, und klicken Sie unter **Servers in der ausgewählten Gruppe** auf **Add**, um den AAA-Server hinzuzufügen.

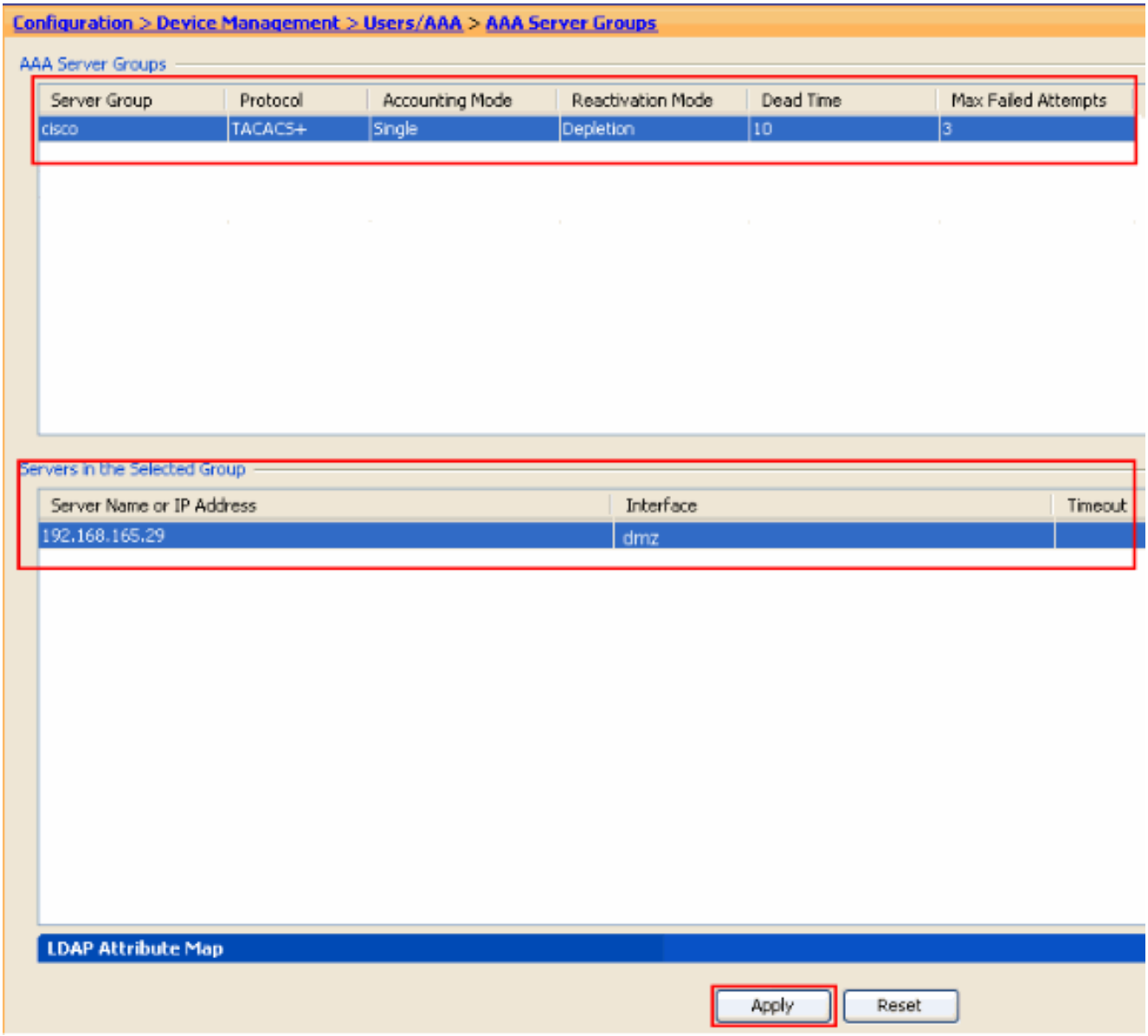


4. Geben Sie die **AAA-Serverdetails** im Fenster **AAA-Server hinzufügen** wie gezeigt ein. Die verwendete Servergruppe ist

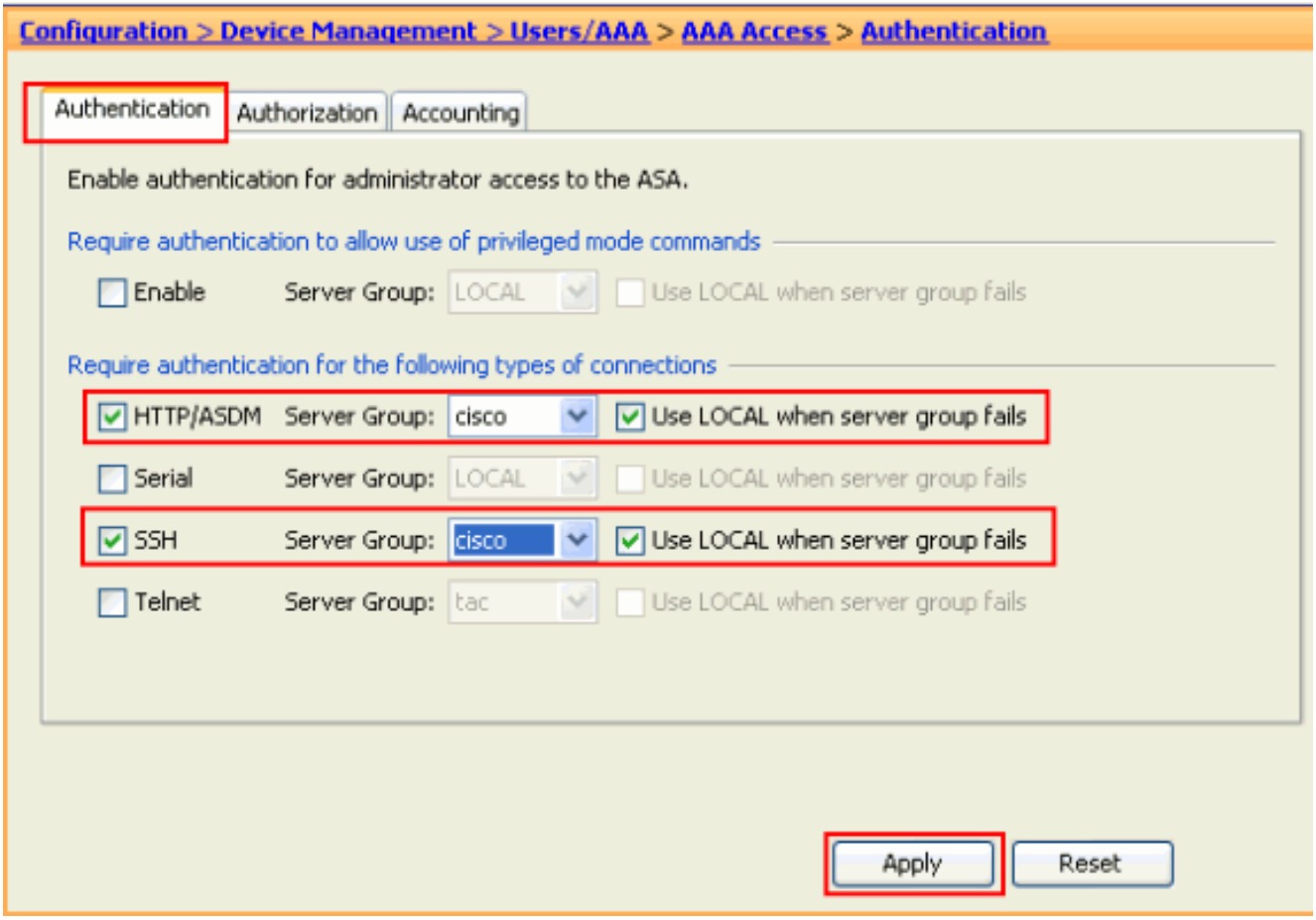


cisco.Klicken Sie auf **OK** und dann auf **Übernehmen**.Sie sehen die **AAA-Servergruppe** und den auf der ASA konfigurierten **AAA-Server**.

5. Klicken Sie auf **Übernehmen**.



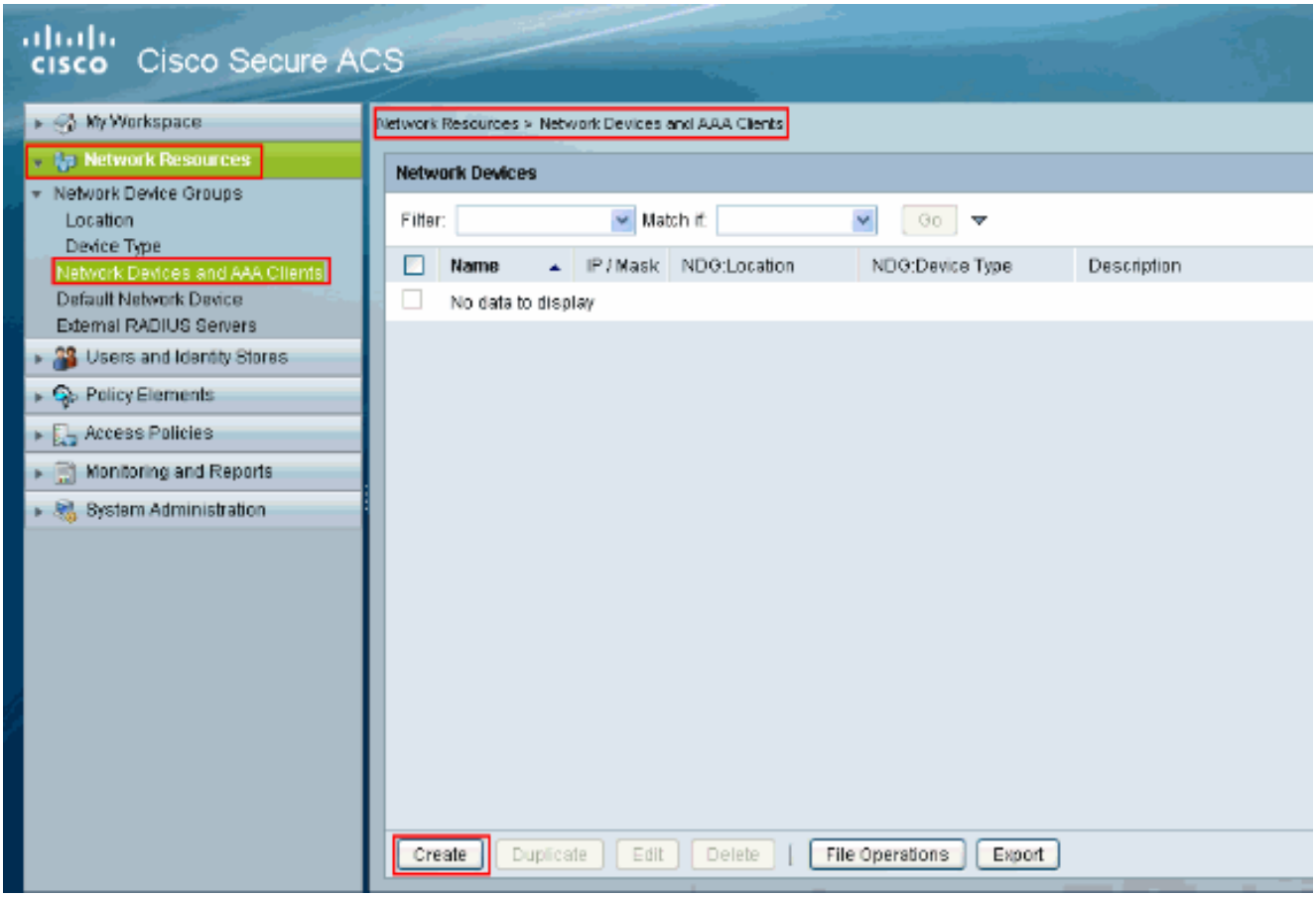
6. Wählen Sie **Configuration > Device Management > Users/AAA > AAA Access > Authentication aus,** und aktivieren Sie die Kontrollkästchen neben **HTTP/ASDM** und **SSH**. Wählen Sie dann **cisco** als Servergruppe aus, und klicken Sie auf **Apply**.



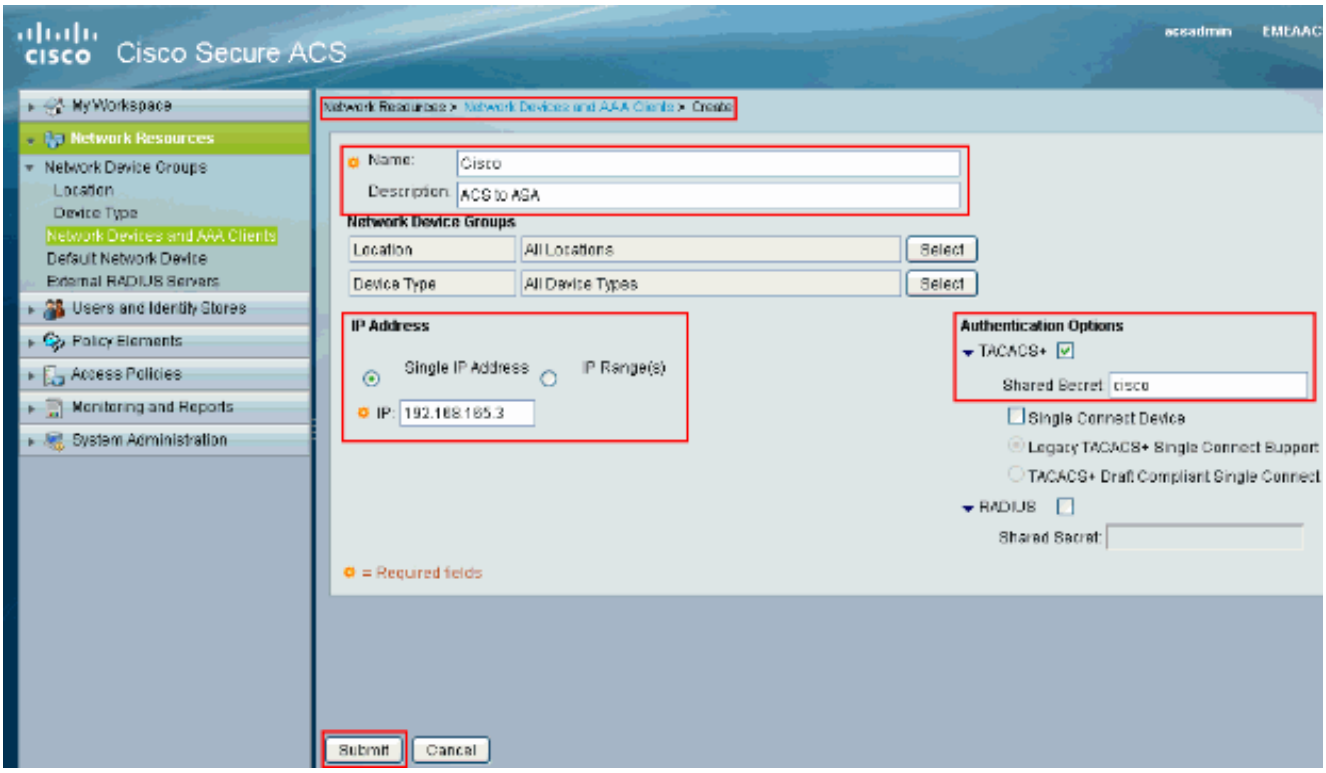
Konfigurieren von ACS als TACACS-Server

Führen Sie dieses Verfahren aus, um den ACS als TACACS-Server zu konfigurieren:

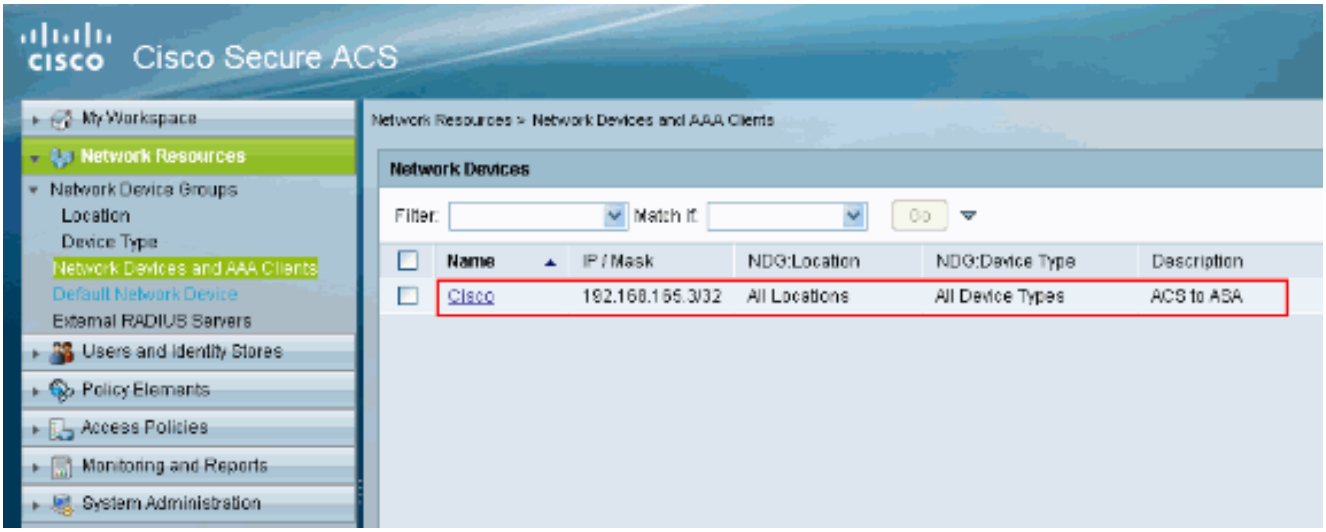
1. Wählen Sie **Network Resources > Network Devices and AAA Clients (Netzwerkressourcen > Netzwerkgeräte und AAA-Clients) aus,** und klicken Sie auf **Create (Erstellen)**, um die ASA zum ACS-Server
hinzuzufügen.



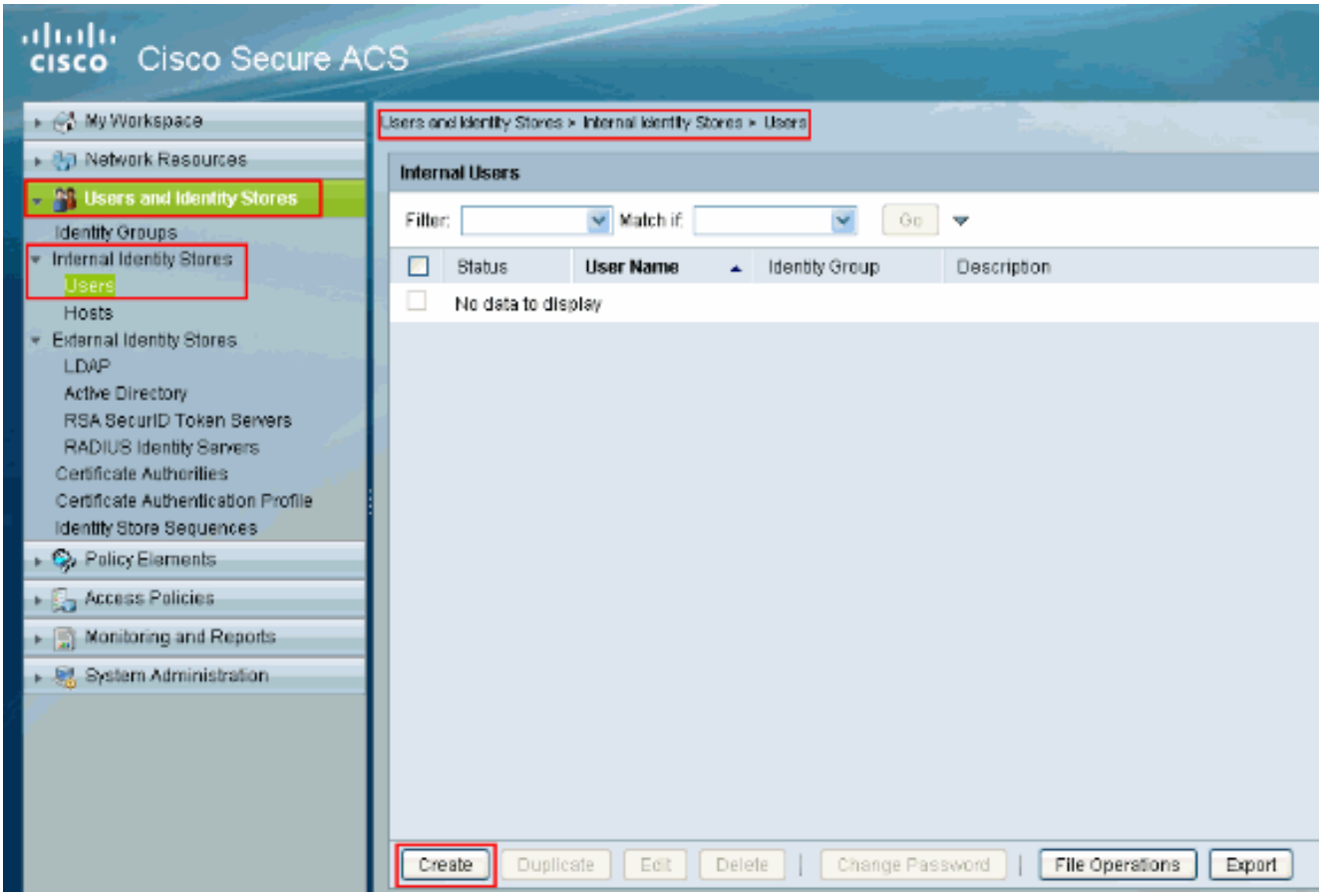
2. Geben Sie die erforderlichen Informationen zum **Client** (hier ist ASA der Client) an, und klicken Sie auf **Senden**. Dadurch kann die ASA zum ACS-Server hinzugefügt werden. Die Details umfassen die **IP-Adresse** der ASA und die Details des **TACACS-Servers**.



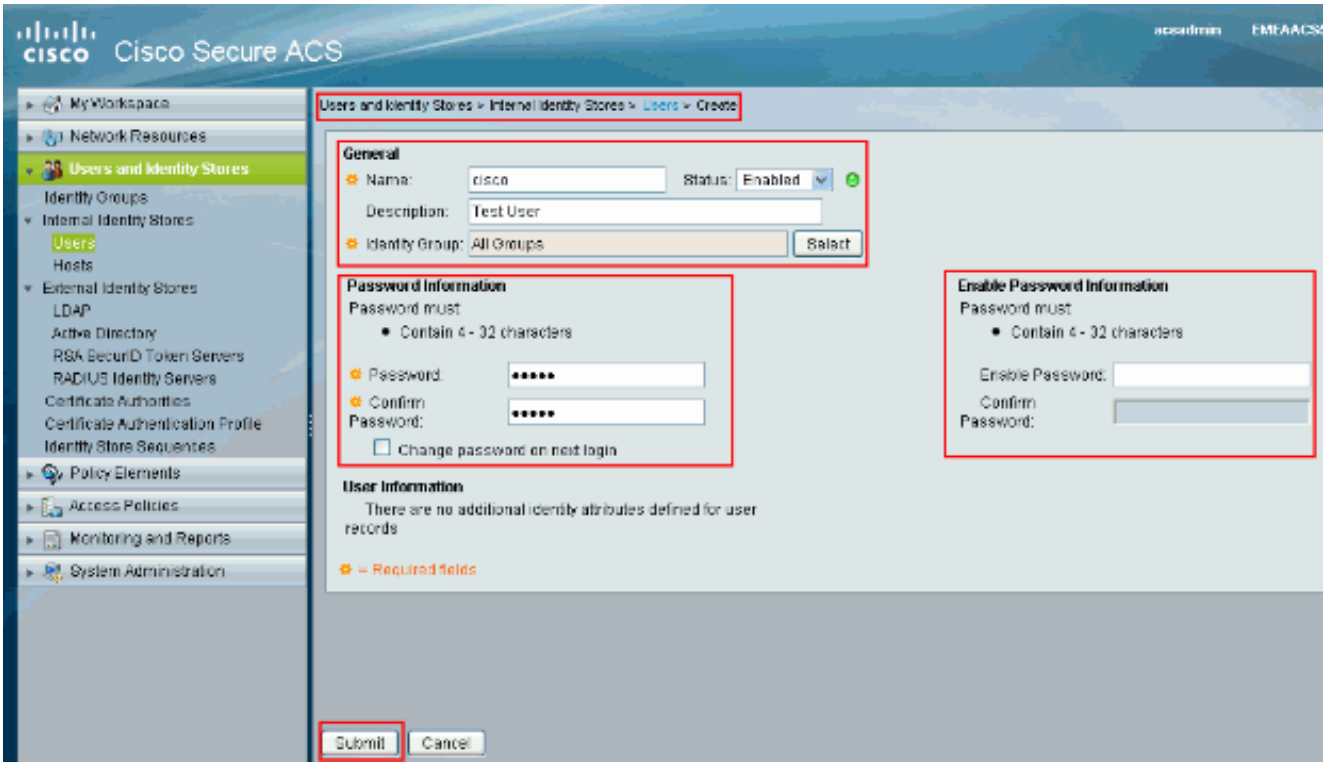
Sie sehen, dass der Client **Cisco** dem ACS-Server hinzugefügt wird.



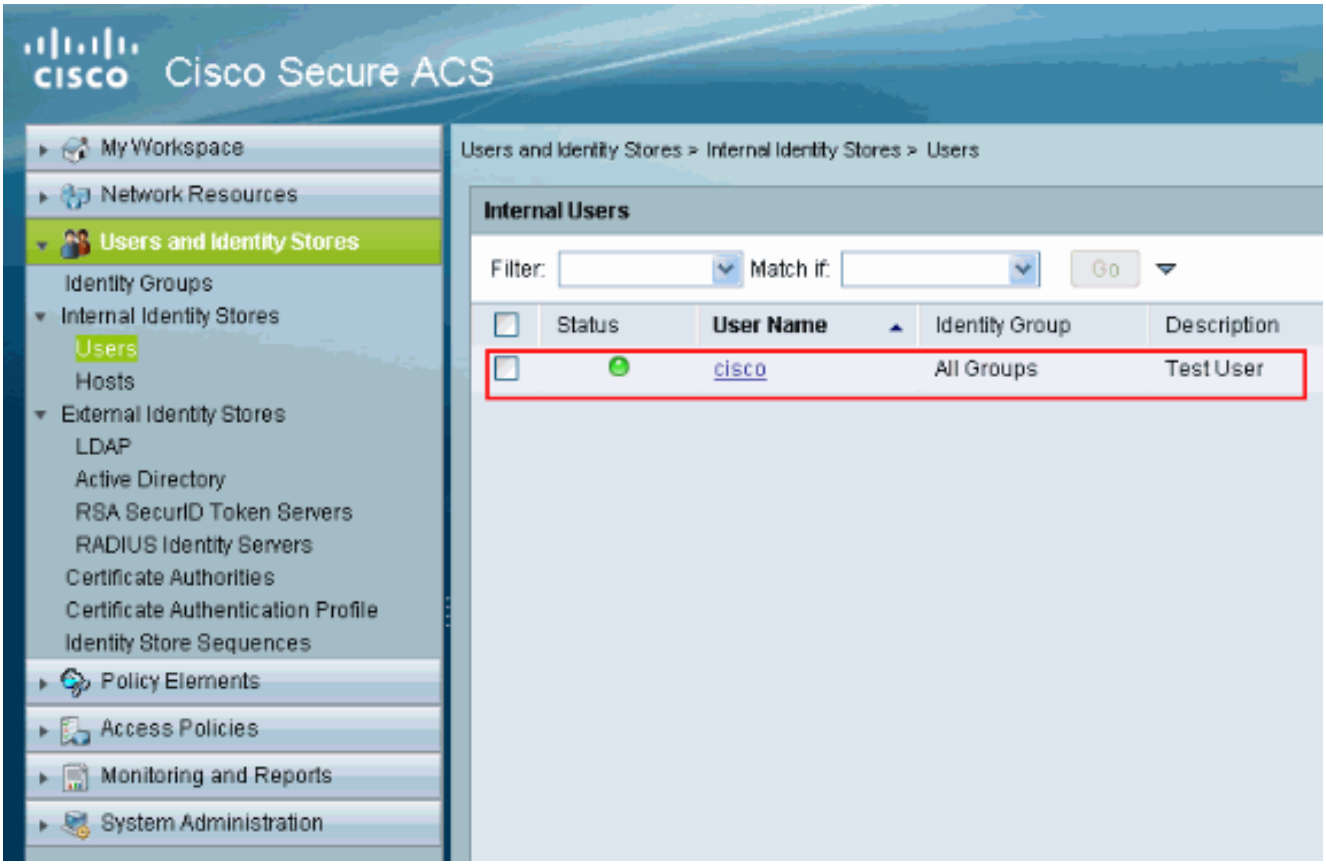
3. Wählen Sie **Benutzer und Identitätsspeicher > Interne Identitätsdaten > Benutzer** und klicken Sie auf **Erstellen**, um einen neuen Benutzer zu erstellen.



4. Geben Sie den **Namen, das Kennwort und die** Informationen **zum Aktivieren des Kennworts an**. **Kennwort aktivieren** ist **optional**. Wenn Sie fertig sind, klicken Sie auf **Senden**.



Sie sehen, dass der Benutzer **cisco** dem ACS-Server hinzugefügt wird.

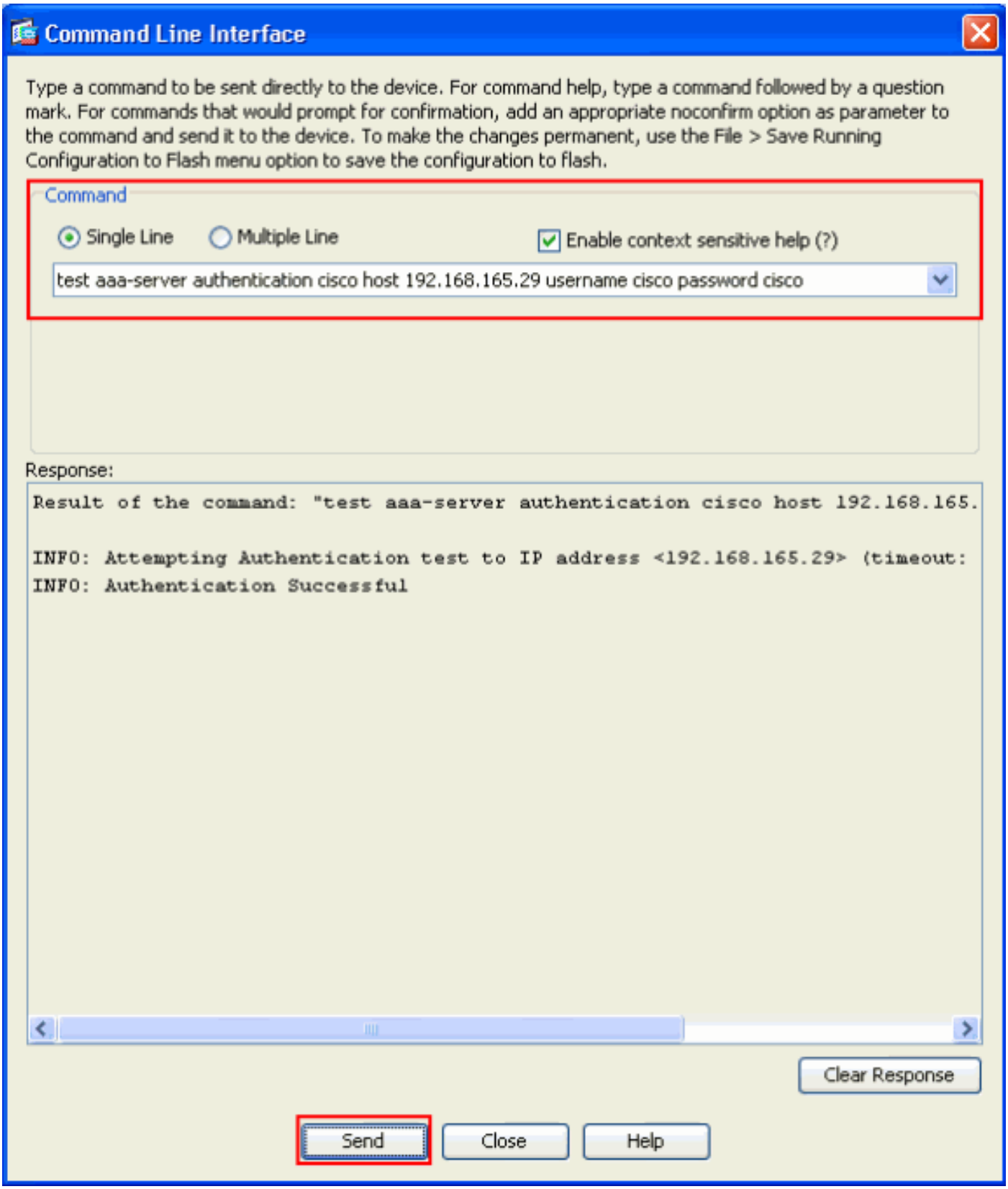


Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Verwenden Sie den Befehl **cisco password cisco** überprüfen **mit der neuesten aaa-server-Authentifizierung cisco host 192.168.165.29**, um zu überprüfen, ob die Konfiguration ordnungsgemäß funktioniert. Dieses Image zeigt, dass die Authentifizierung erfolgreich ist und der

Benutzer, der eine Verbindung zur ASA herstellt, vom ACS-Server authentifiziert wurde.



Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Fehlerbehebung

Fehler: AAA-Markierung von TACACS+-Server x.x.x.x in AAA-Servergruppen-

Taktiken als FEHLGESCHLAGEN

Diese Meldung bedeutet, dass die Cisco ASA die Verbindung zum x.x.x-Server verloren hat. Stellen Sie sicher, dass Sie über eine gültige Verbindung auf TCP 49 mit Server x.x.x.x von der ASA verfügen. Bei einer Netzwerklatenz können Sie die Zeitüberschreitung auf dem ASA-Server für TACACS+ von 5 auf die gewünschte Anzahl von Sekunden erhöhen. Die ASA sendet keine Authentifizierungsanfrage an den FAILED-Server x.x.x.x. Es wird jedoch den nächsten Server in den AAA-Server-Gruppen-Taktiken verwenden.

Zugehörige Informationen

- Support-Seite für Cisco Adaptive Security Appliances der Serie ASA 5500
- Cisco Adaptive Security Appliances der Serie ASA 5500 - Befehlsreferenzen
- Cisco Adaptive Security Device Manager
- Support-Seite für IPsec-Aushandlung/IKE-Protokolle
- Cisco Secure Access Control Server für Windows
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems