ASA 8.3： ACS 5.X を使用した TACACS 認証

目次

概要

このドキュメントでは、ユーザのネットワーク アクセスを認証するためのセキュリティ アプライアンスの設定方法について説明します。

前提条件

要件

このドキュメントでは、適応型セキュリティ アプライアンス（ASA）が完全に動作していて、Cisco Adaptive Security Device Manager（ASDM）か CLI 設定を変更できるように設定されていることを想定しています。

注: デバイス を ASDM によってリモートで設定できるようにする方法については、「ASDM での HTTPS アクセスの許可」を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 適応型セキュリティ アプライアンス ソフトウェア バージョン 8.3 以降
- Adaptive Security Device Manager バージョン 6.3 以降
- Cisco Secure Access Control Server 5.x

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

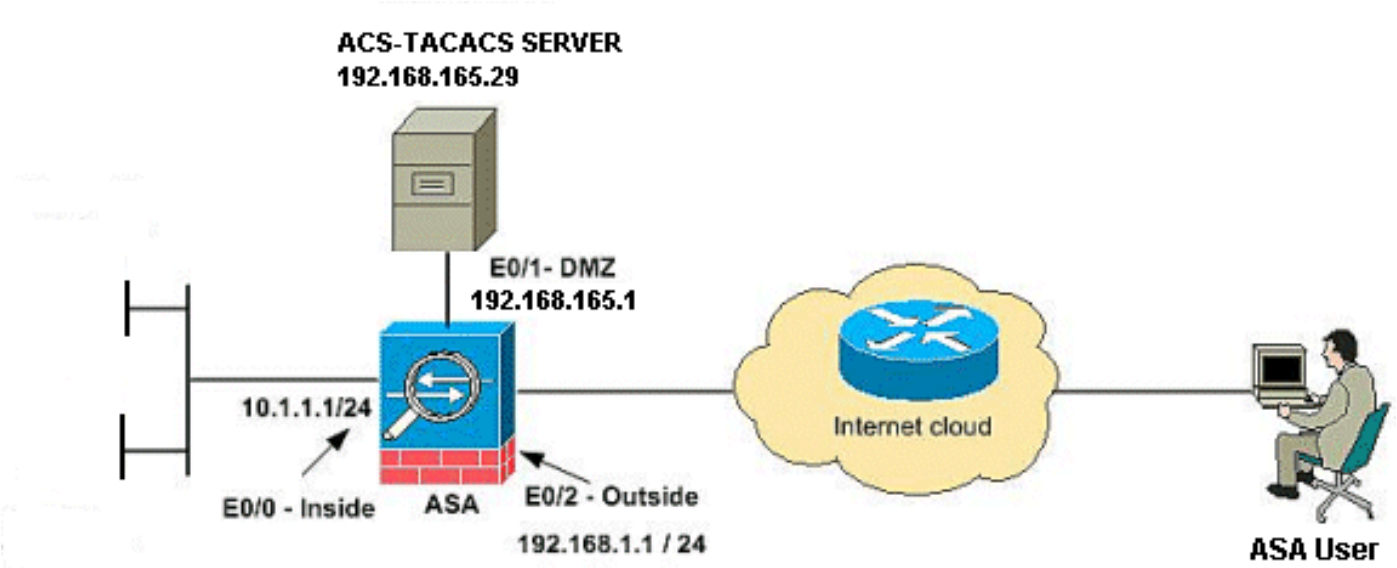
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらは RFC 1918 でのアドレスであり、ラボ環境で使用されたものです。

CLI を使用して ACS サーバから ASA の認証を設定する方法

ASA で ACS サーバから認証するには、次の設定を実行します。

```
!--- 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
```

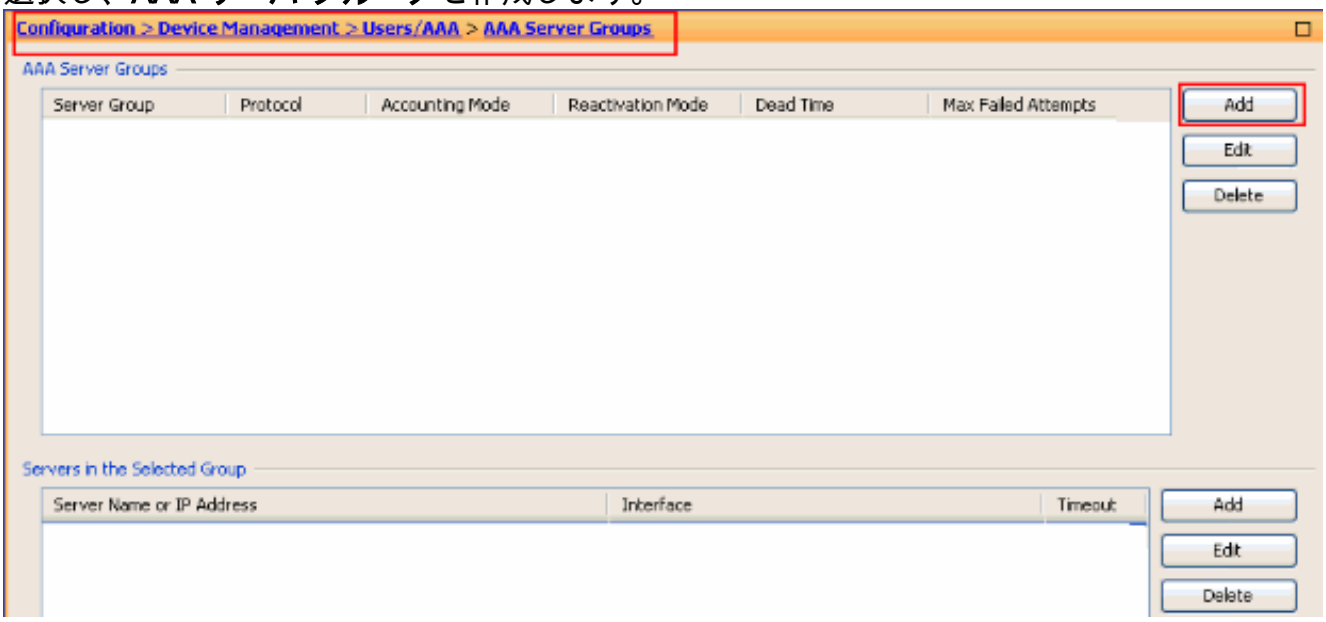
注: ACS が使用できない場合に、ローカル認証で ASDM にアクセスするには、username cisco password cisco privilege 15 コマンドを使用して、ASA にローカル ユーザを作成します。

ASDM を使用して ACS サーバから ASA の認証を設定する方法

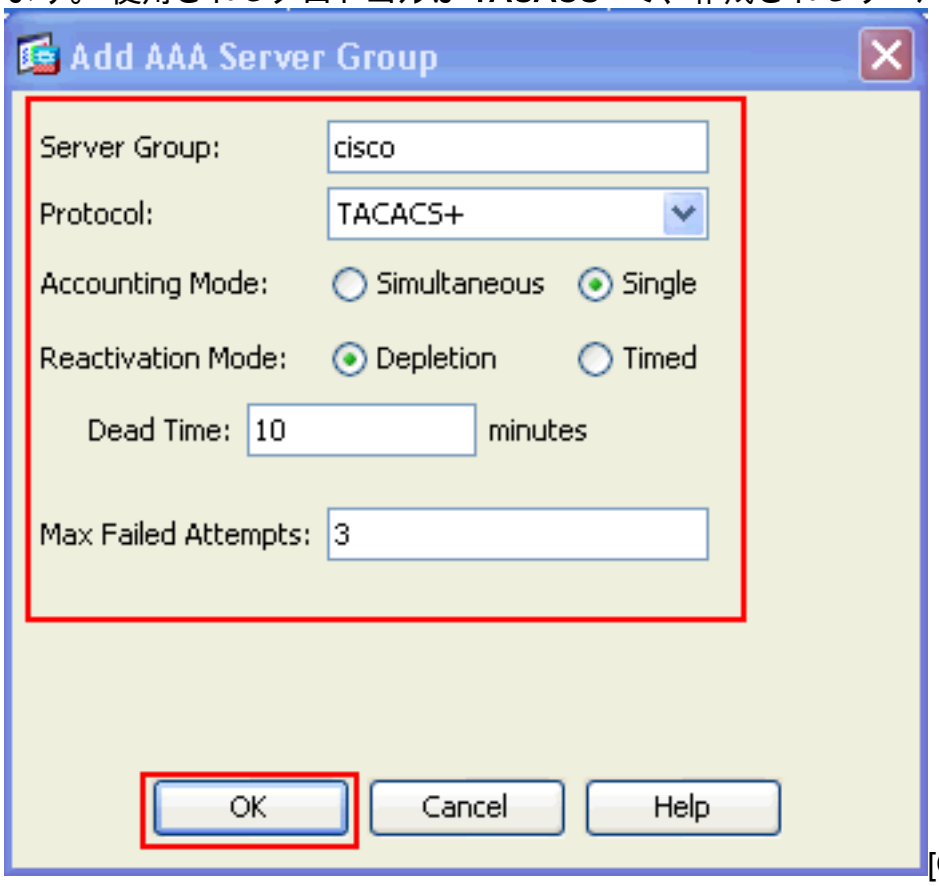
ASDM の手順

ASA で ACS サーバから認証するには、次の手順を実行します。

1. [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] > [Add] の順に選択し、**AAA サーバ グループ**を作成します。



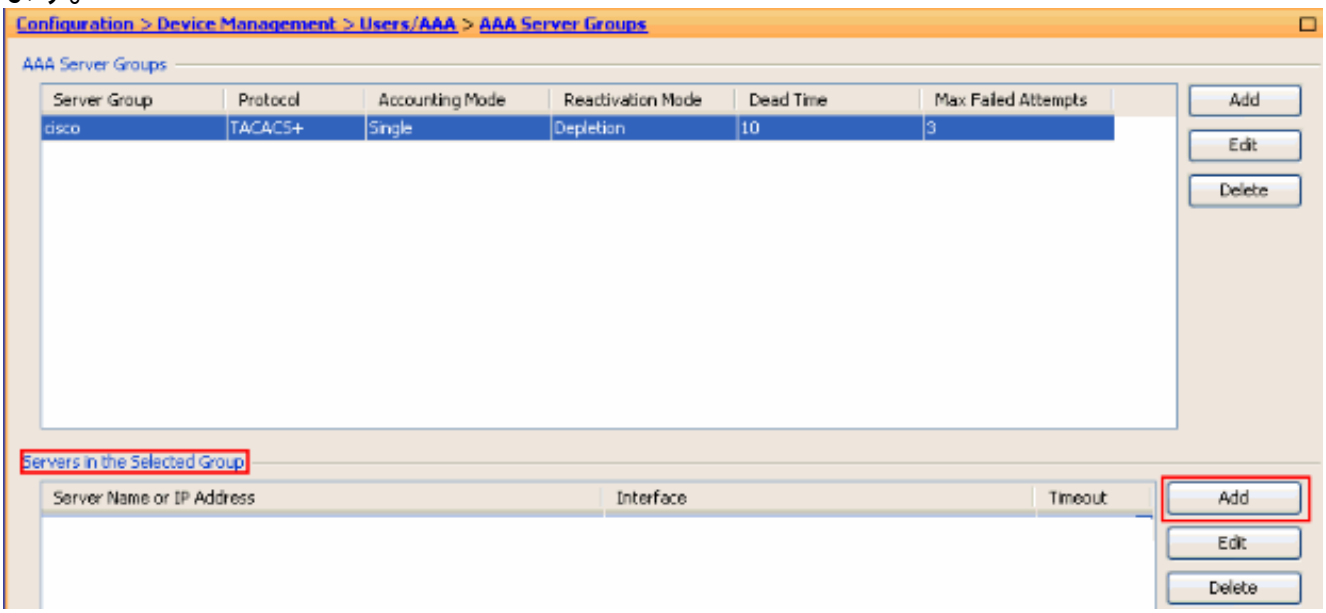
2. 次に示すように、[Add AAA Server Group] ウィンドウに **AAA サーバ グループ**の詳細が表示されます。 使用されるプロトコルは **TACACS+** で、作成されるサーバ グループは **cisco** で



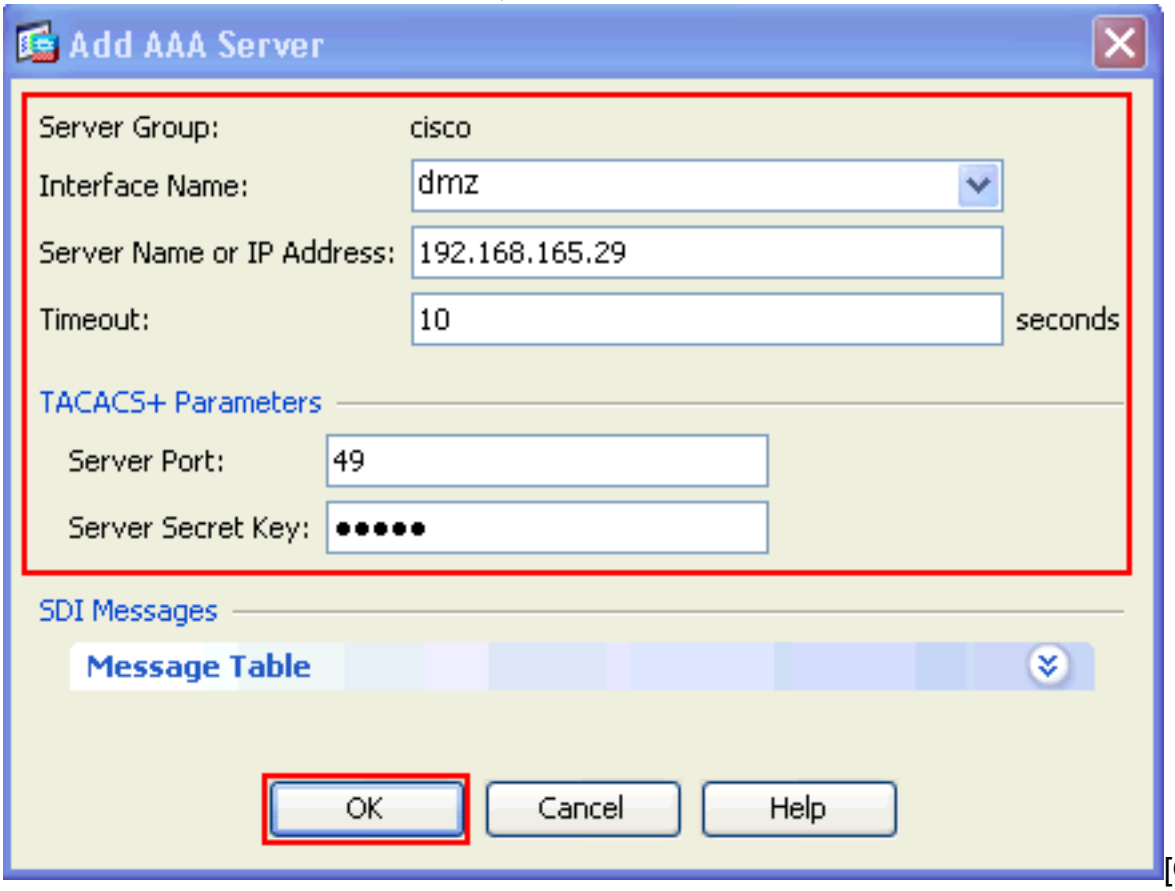
す。[OK] をクリックします

。

3. [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] の順に選択し、[Servers in the Selected Group] の下にある [Add] をクリックして、AAA サーバを追加します。

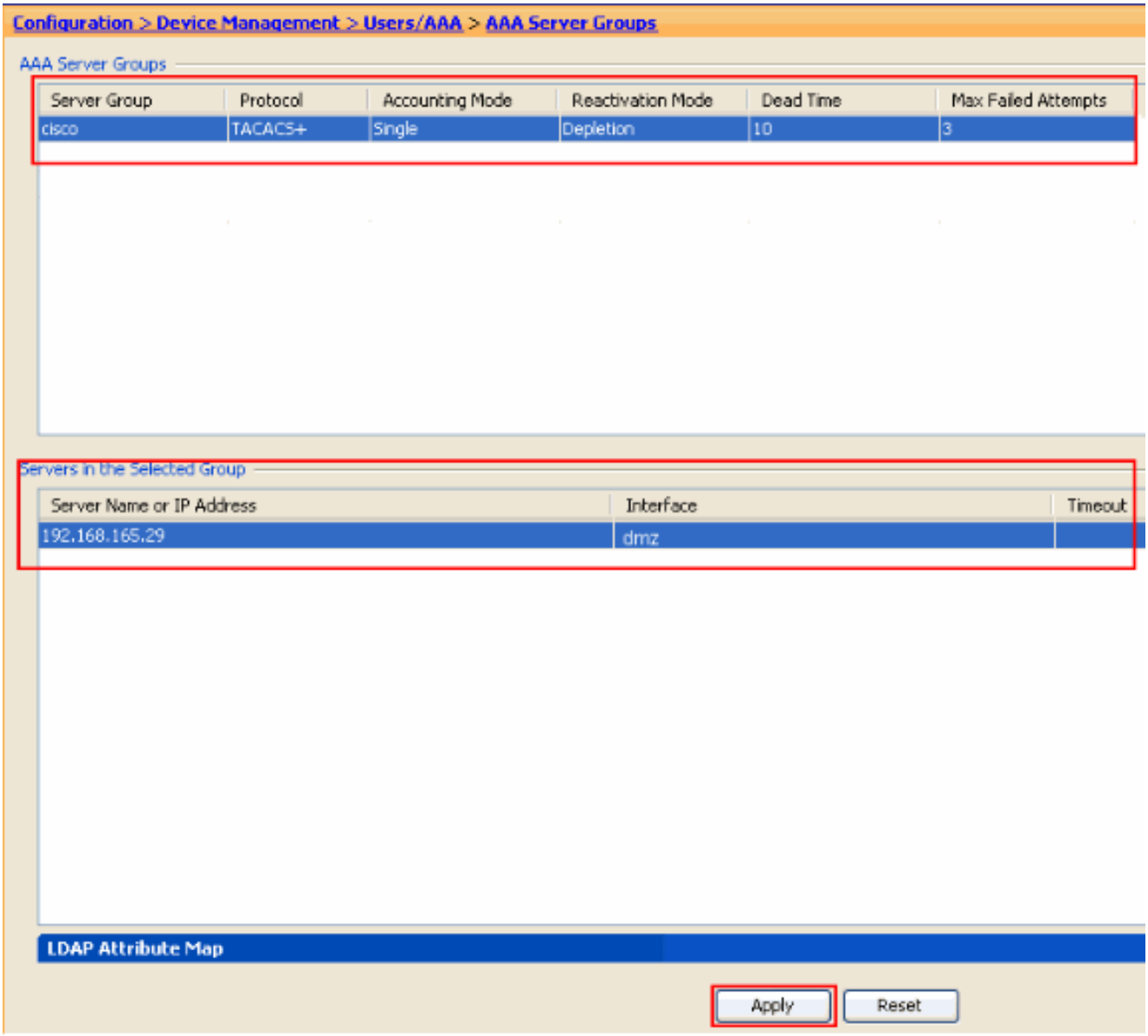


4. 次に示すように、[Add AAA Server] ウィンドウに **AAA サーバ**の詳細が表示されます。 使用されるサーバ グループは **cisco** です。

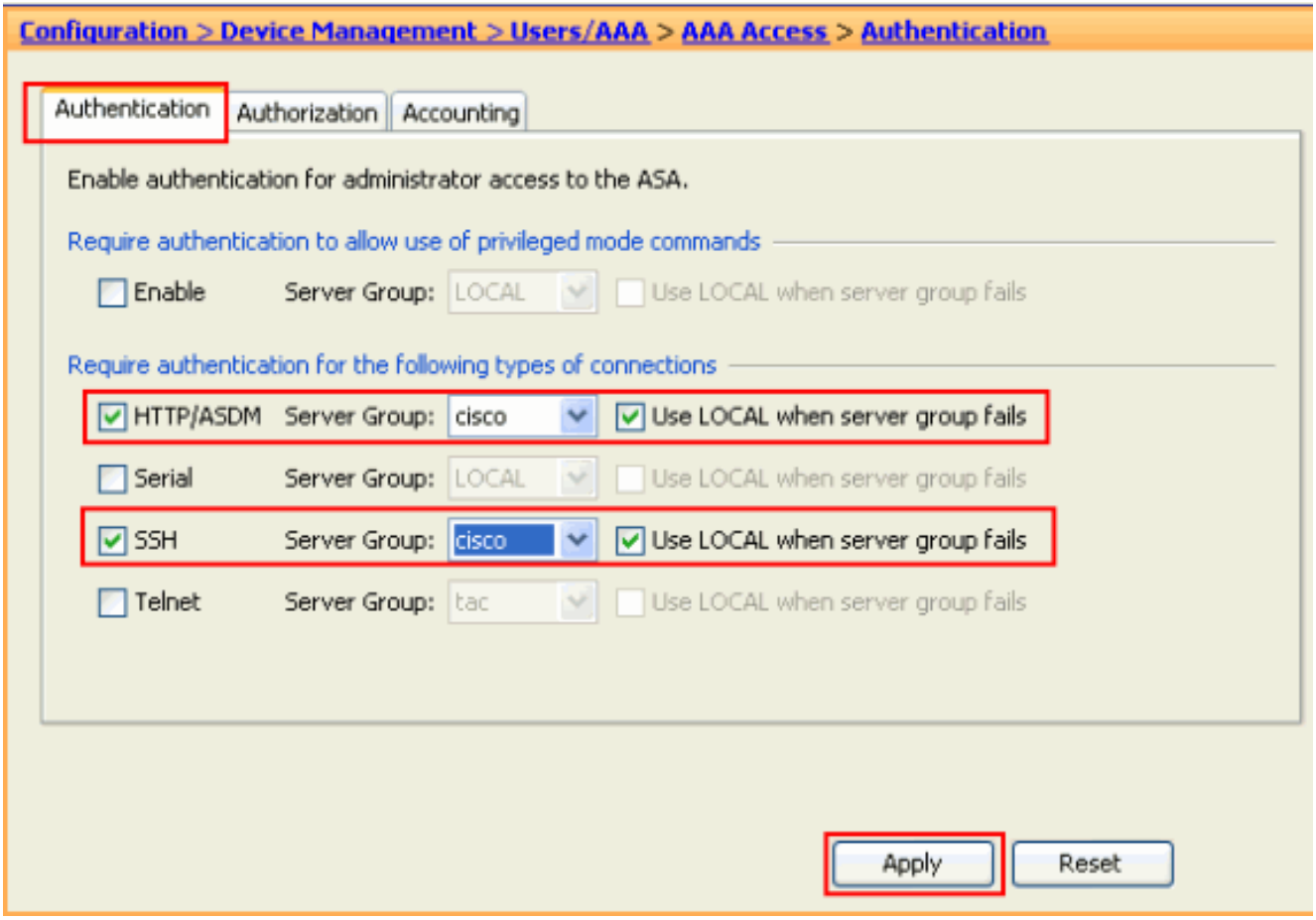


[OK] をクリックし、[Apply] をクリックします。**AAA サーバ グループ**と **AAA サーバ** が ASA に設定されます。

5. [Apply] をクリックします。



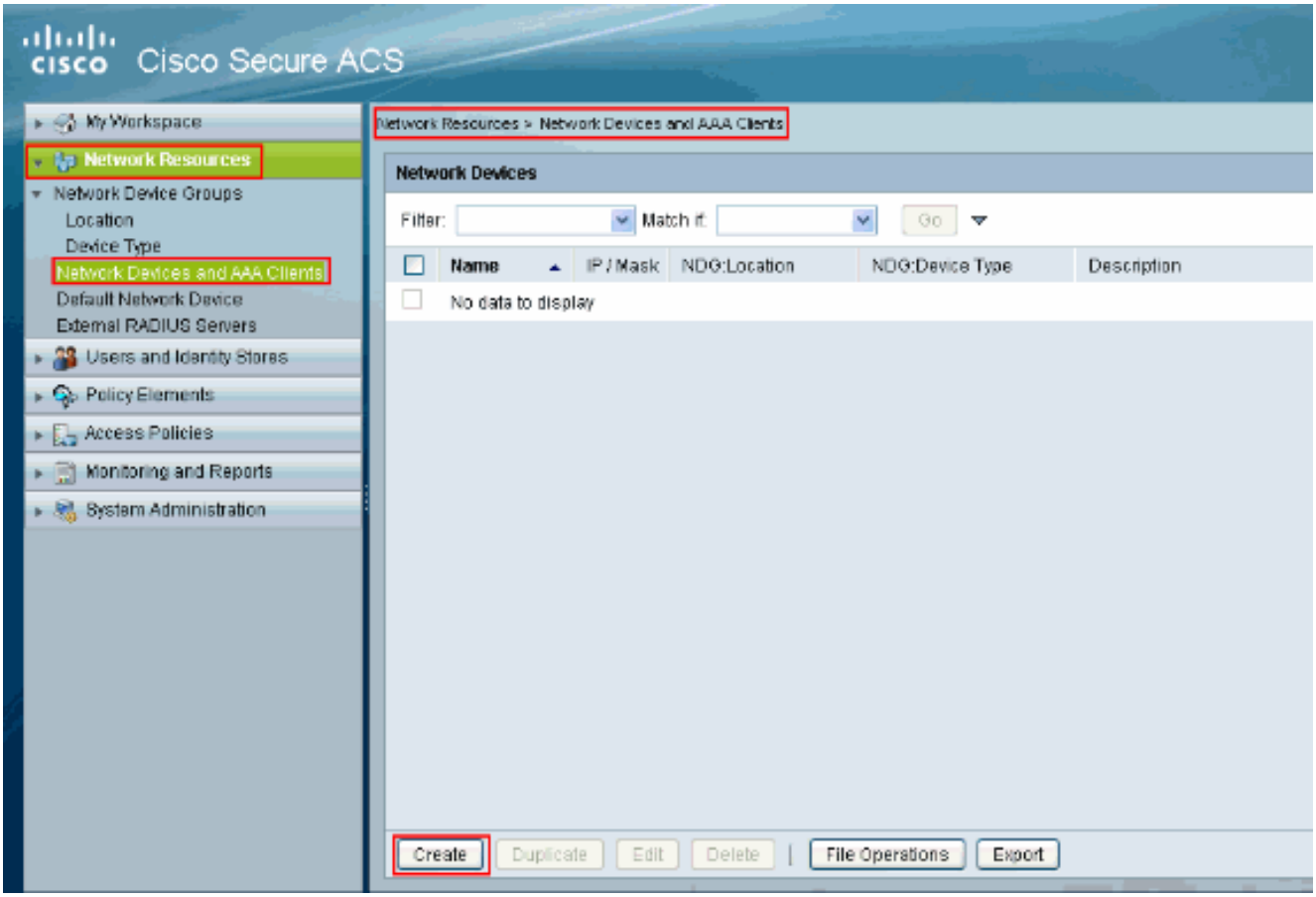
6. [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication] の順に選択し、[HTTP/ASDM] と [SSH] の横のチェック ボックスをオンにします。 次に、サーバ グループとして **cisco** を選択し、[Apply] をクリックします。



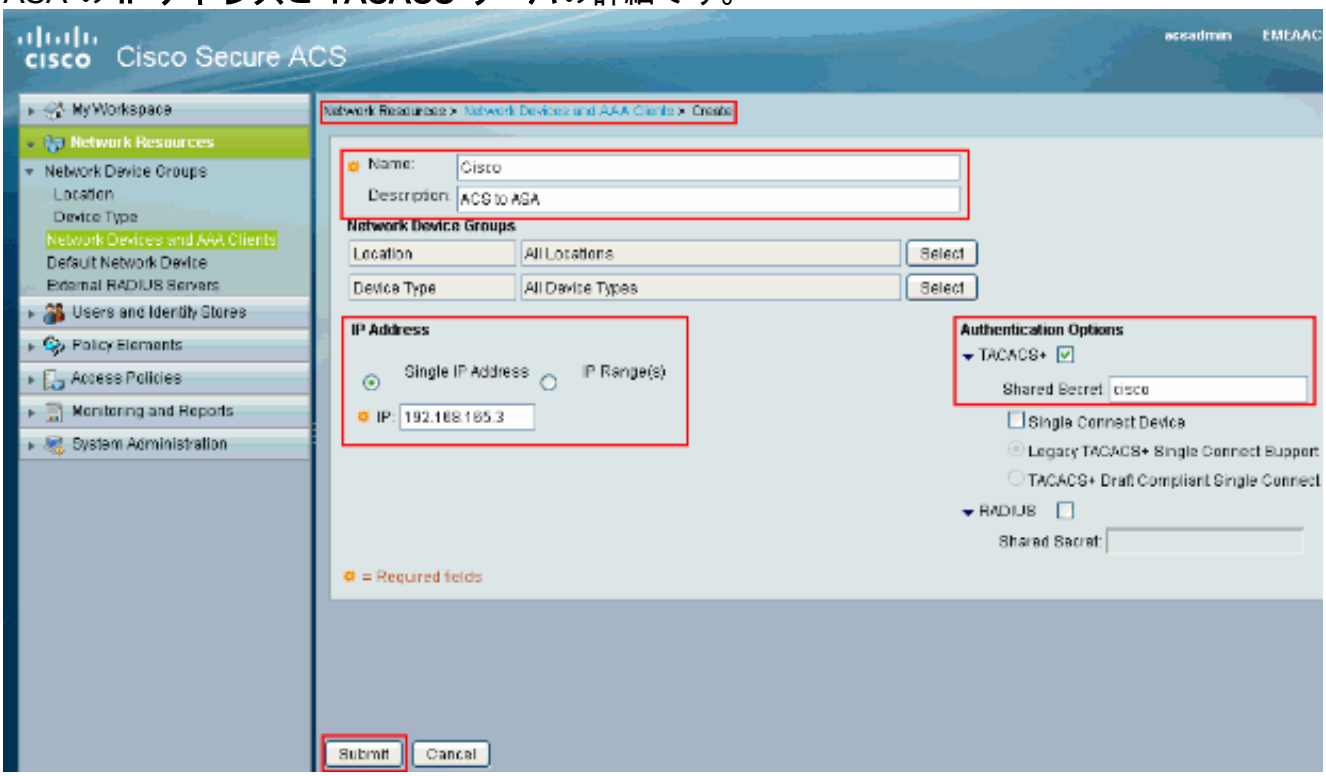
ACS を TACACS サーバとして設定する方法

ACS を TACACS サーバとして設定するには、次の手順を実行します。

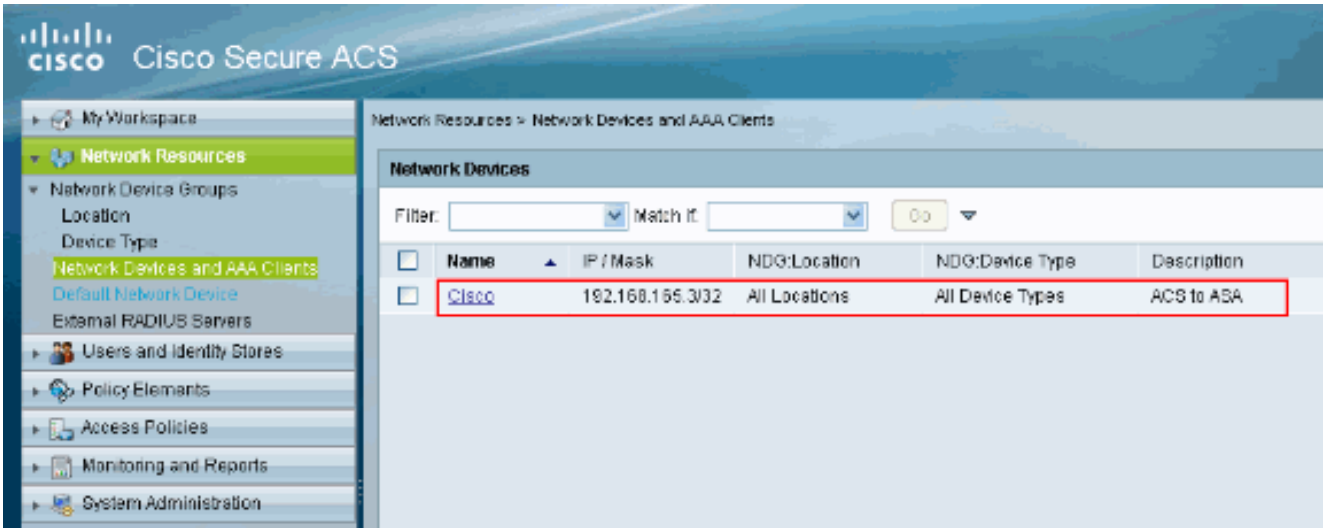
1. [Network Resources] > [Network Devices and AAA Clients] の順に選択し、[Create] をクリックして、ASA を ACS サーバに追加します。



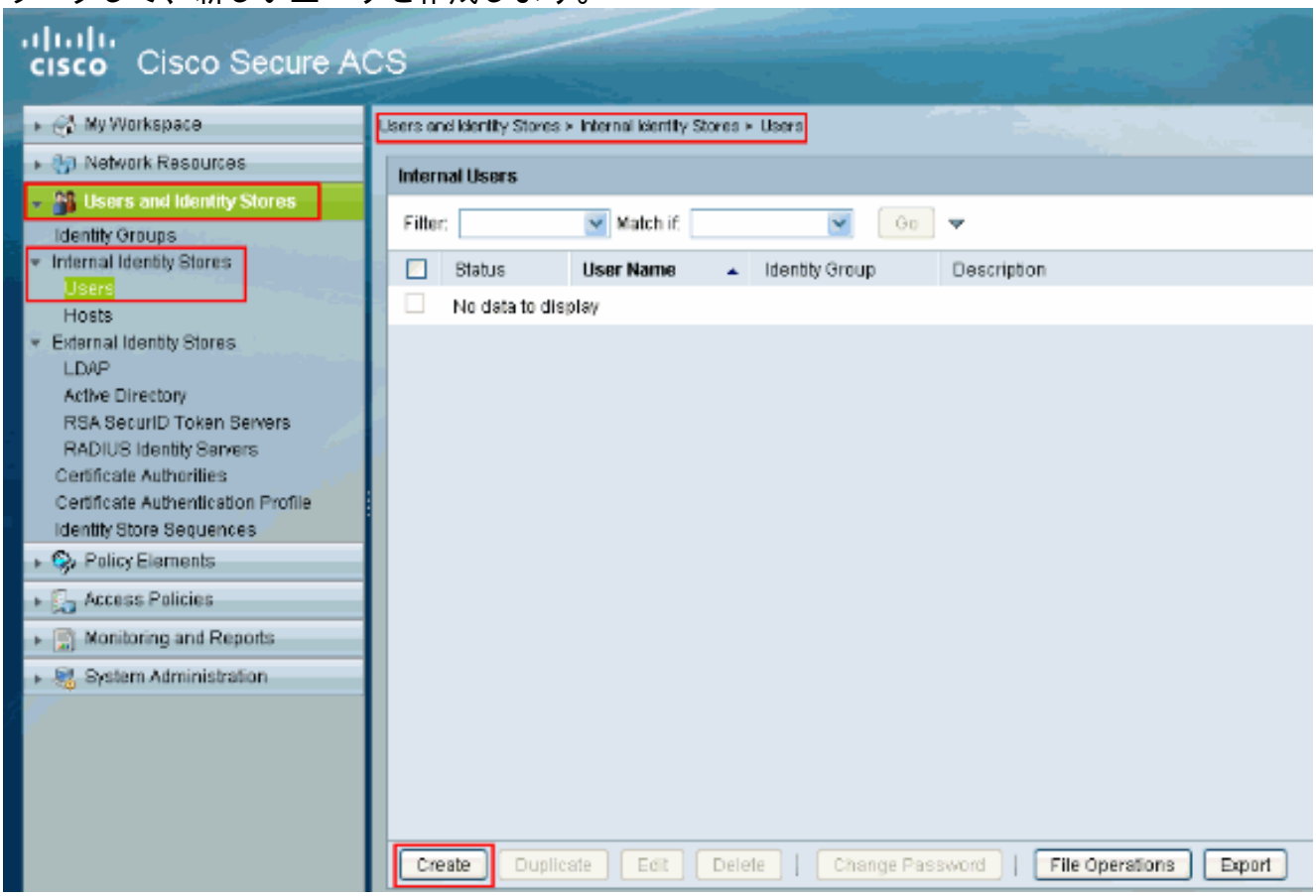
2. **クライアント**（ここでは ASA がクライアント）について必要な情報を指定し、[Submit] をクリックします。 これで、ASA を ACS サーバに追加できます。 詳細に含まれるのは、ASA の **IP アドレス**と **TACACS サーバ**の詳細です。



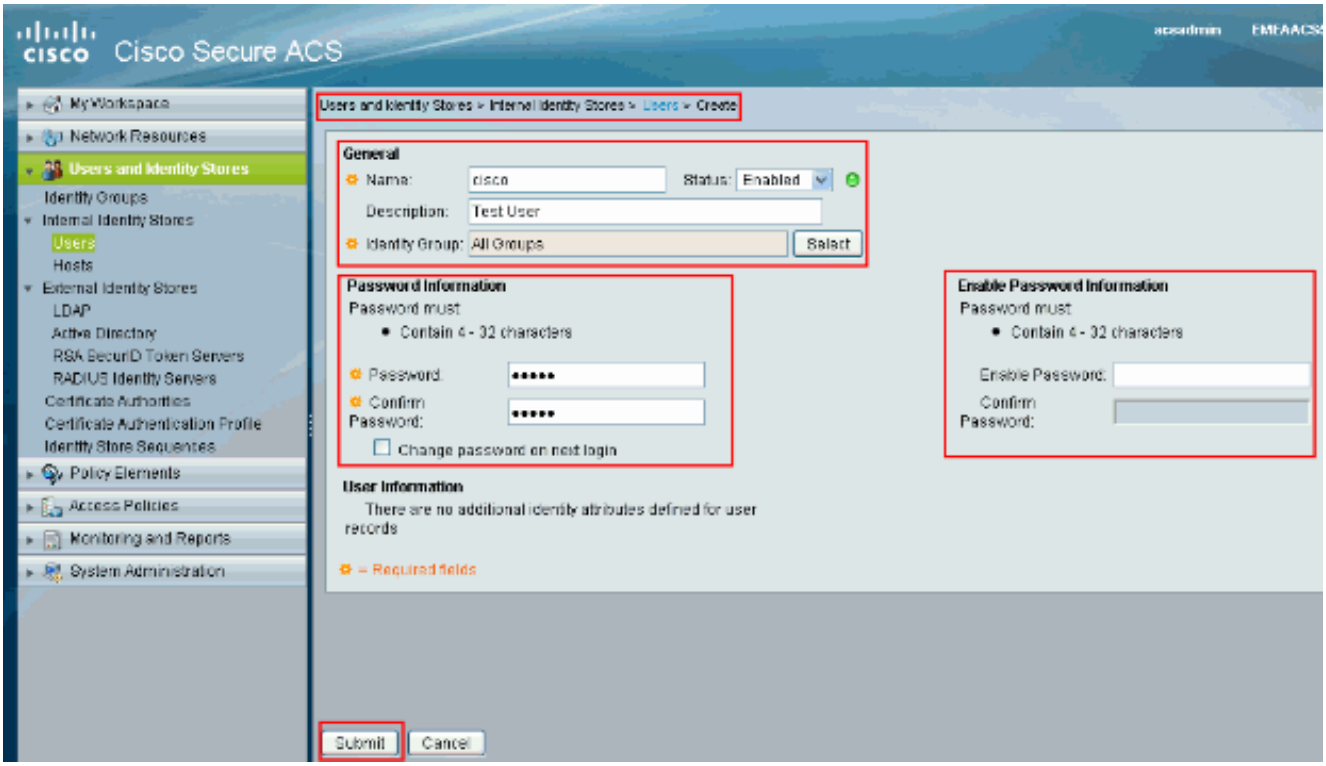
クライアント **Cisco** が ACS サーバに追加されています。



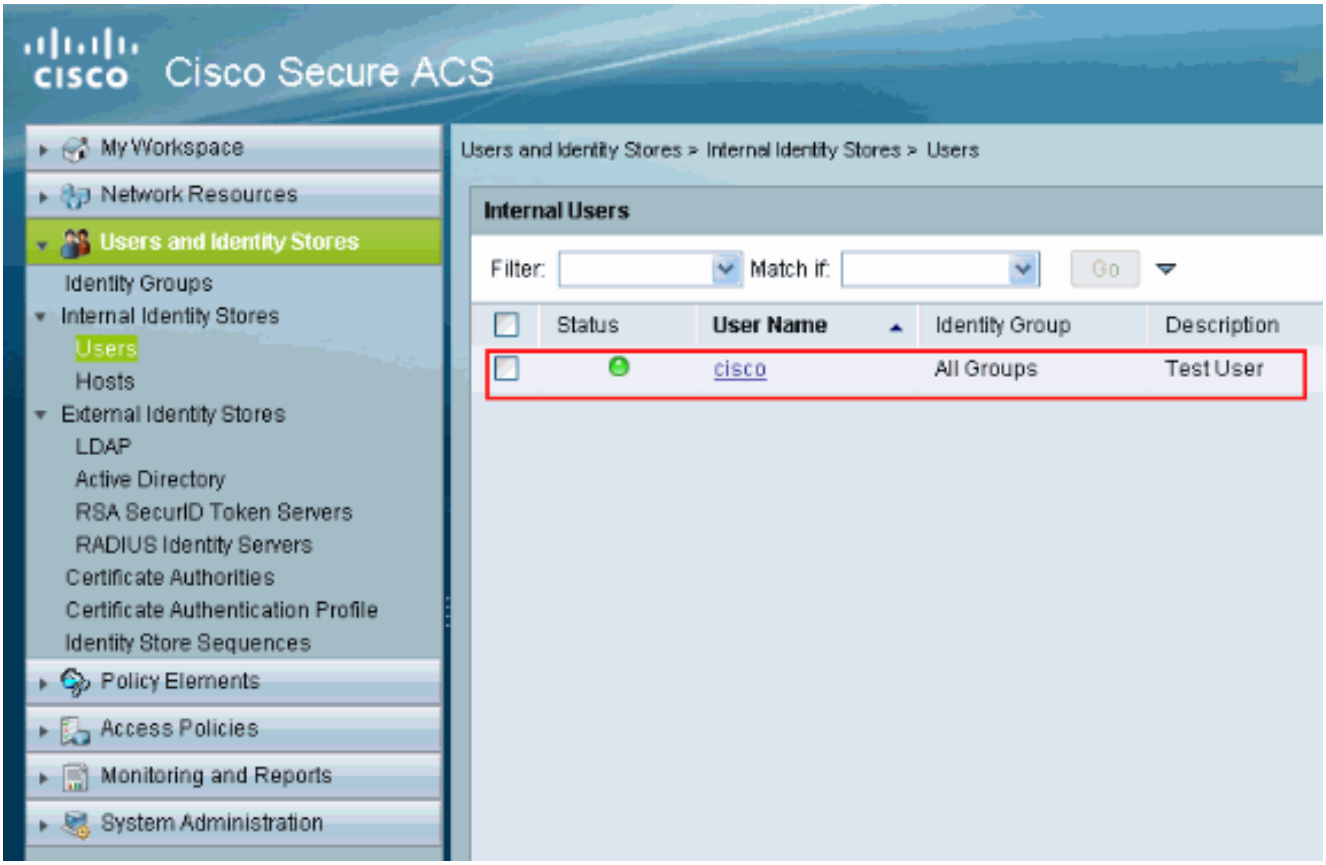
3. [Users and Identity stores] > [Internal Identity Stores] > [Users] の順に選択し、[Create] をクリックして、新しいユーザを作成します。



4. [Name]、[Password] および [Enable Password] に必要な情報を指定します。 [Enable Password] は**オプション**です。 終了したら、[Submit] をクリックします。



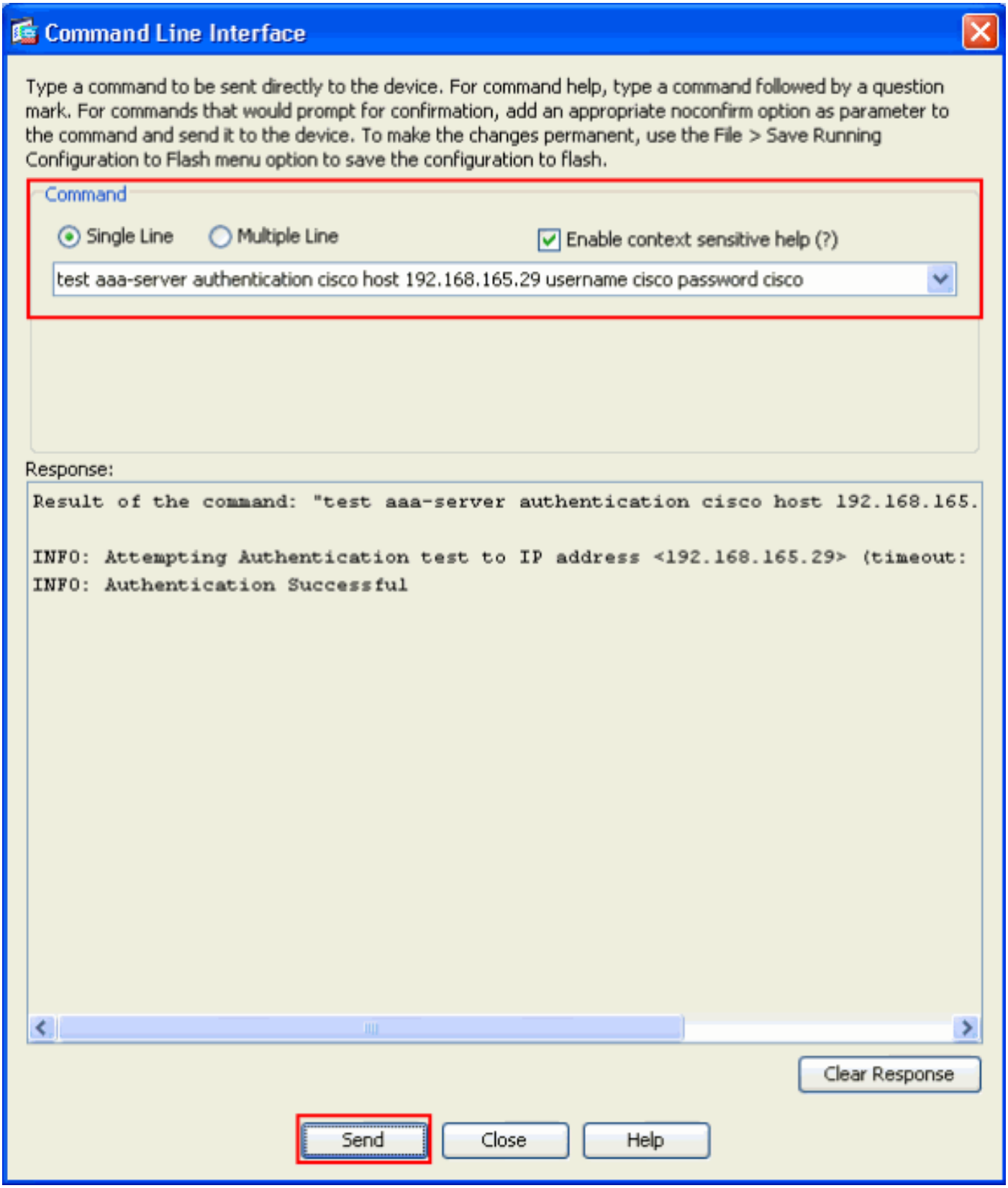
ユーザ cisco が ACS サーバに追加されています。



確認

ここでは、設定が正常に動作していることを確認します。

test aaa-server authentication cisco host 192.168.165.29 username cisco password cisco コマンドを使用し、設定が正しく動作するかどうかを確認します。 次の図は、認証が成功し、ASA に接続しているユーザが ACS サーバによって認証されていることを示しています。



Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

トラブルシューティング

エラー： AAA Marking TACACS+ server x.x.x.x in aaa-server group tacacs as FAILED

このメッセージは、Cisco ASA と x.x.x.x サーバとの接続が失われたことを意味します。 ASA からサーバ x.x.x.x への有効な接続が tcp 49 にあることを確認します。 ネットワークの遅延が発生する場合は、ASA で TACACS+ サーバのタイムアウトを 5 秒から必要な秒数に増やすこともできます。 ASA は FAILED サーバ x.x.x.x に認証要求を送信しませんが、 aaa-server group tacacs の次のサーバを使用します。

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスに関するサポート ページ
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス、コマンド リファレンス
- Cisco Adaptive Security Device Manager
- IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ
- Cisco Secure Access Control Server for Windows
- Requests for Comments (RFC)
- テクニカルサポートとドキュメント - Cisco Systems