ASA 8.3: Autenticación de TACACS usando ACS 5.X

Contenido

Introducción

Este documento proporciona la información sobre cómo configurar el dispositivo de seguridad para autenticar a los usuarios para el acceso a la red.

prerrequisitos

Requisitos

Este documento asume que el dispositivo de seguridad adaptante (ASA) está completamente - operativo y configurado para permitir que el Cisco Adaptive Security Device Manager (ASDM) o el CLI realice los cambios de configuración.

Nota: Refiera a permitir el acceso HTTPS para el ASDM para más información sobre cómo permitir que el dispositivo sea configurado remotamente por el ASDM.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión de software adaptante 8.3 del dispositivo de seguridad de Cisco y posterior
- Versión 6.3 y posterior del Cisco Adaptive Security Device Manager
- Cisco Secure Access Control Server 5.x

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

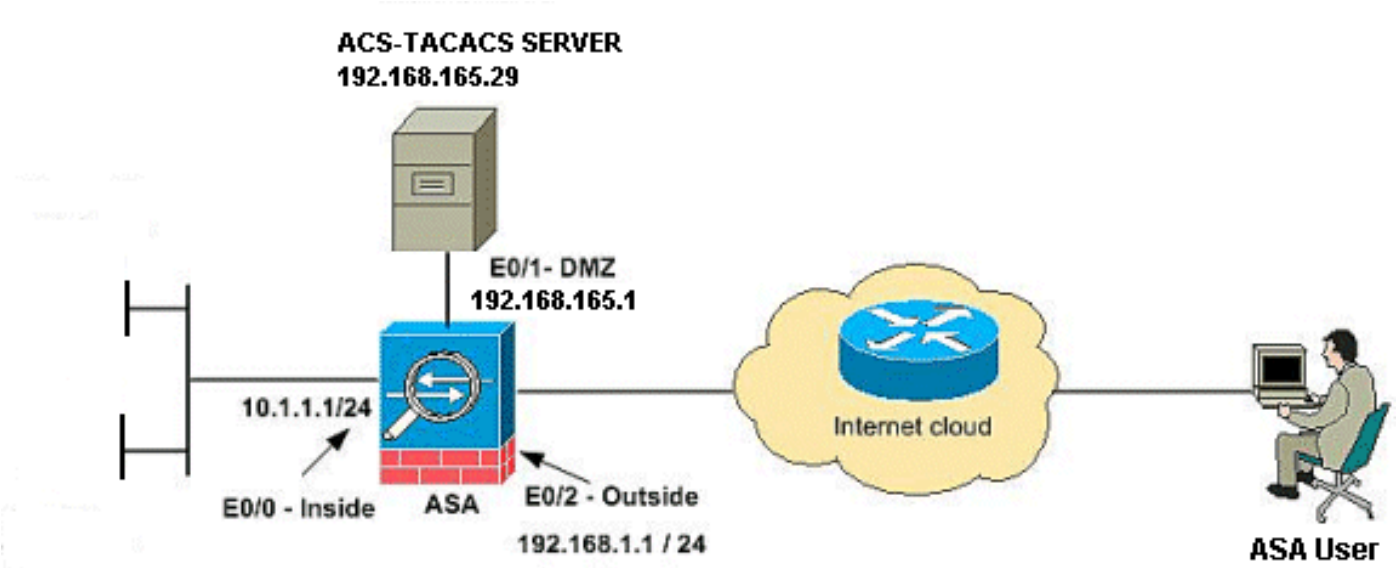
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que fueron utilizadas en un entorno de laboratorio.

Configure el ASA para la autenticación del servidor ACS que usa el CLI

Realice estas configuraciones para el ASA para autenticar del servidor ACS:

```
!--- 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
```

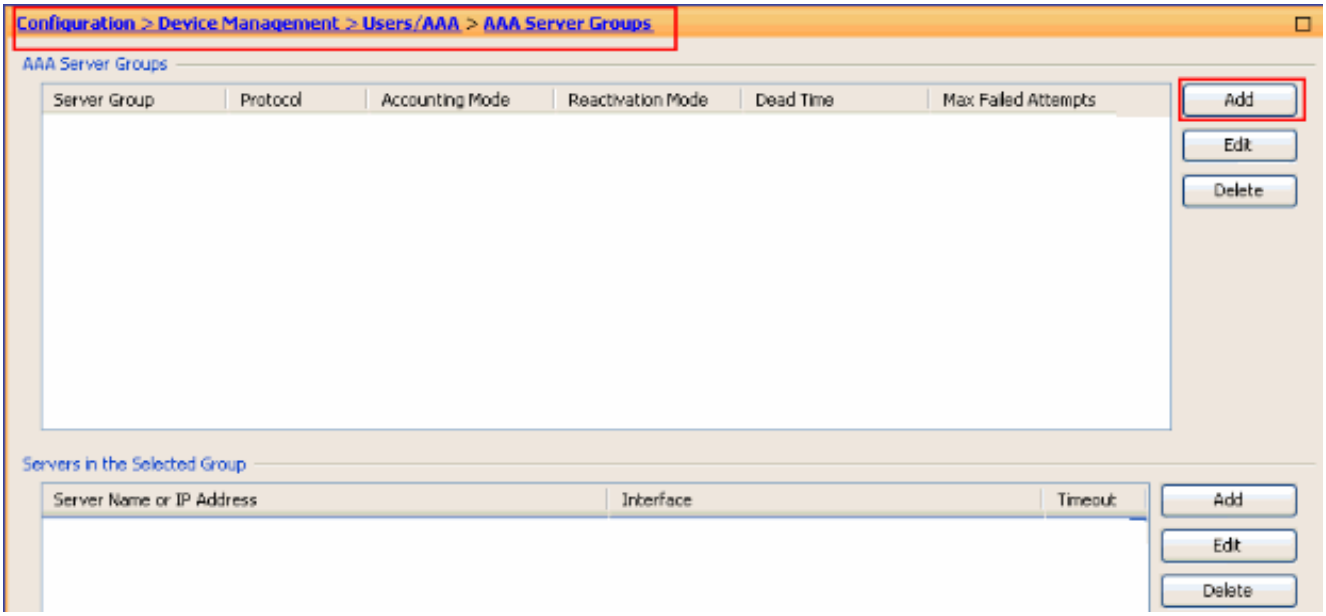
Nota: Cree a un usuario local en el ASA usando el comando del **privilegio 15 de la palabra clave Cisco del nombre de usuario cisco** de acceder el ASDM con la autenticación local cuando el ACS no está disponible.

Configure el ASA para la autenticación del servidor ACS que usa el ASDM

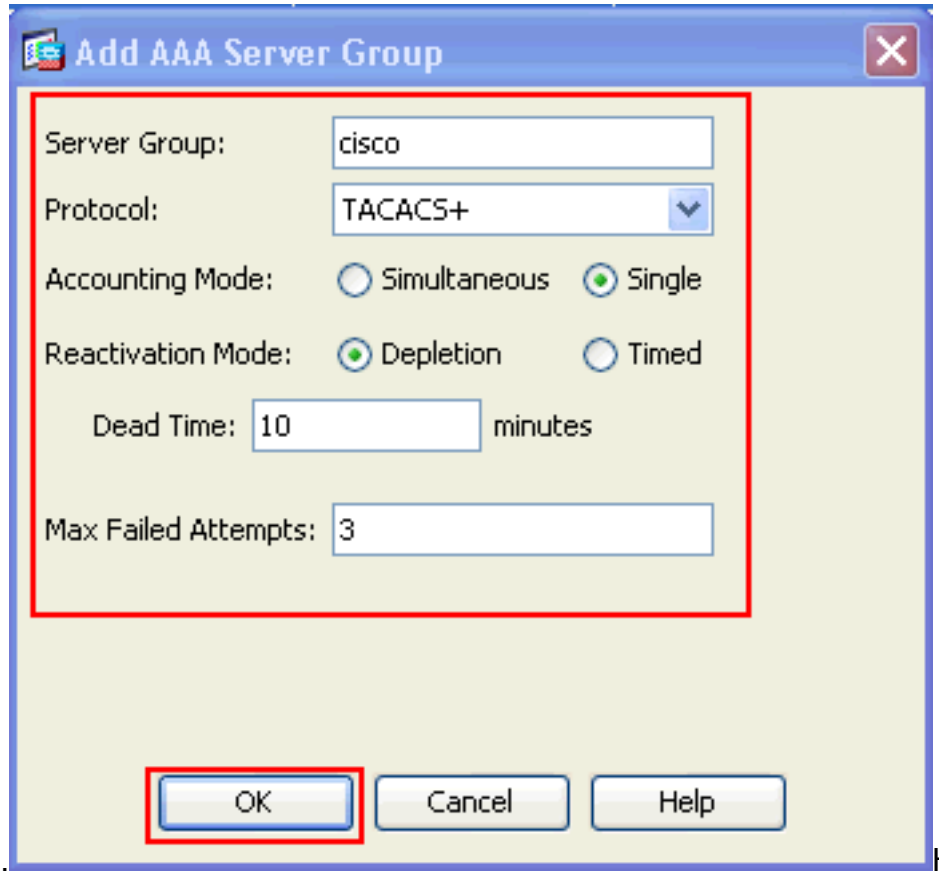
Procedimiento del ASDM

Complete estos pasos para configurar el ASA para la autenticación del servidor ACS:

1. Elija la **configuración > la Administración de dispositivos > a los grupos de servidores Users/AAA >AAA > Add** para crear a un **Grupo de servidores AAA**.

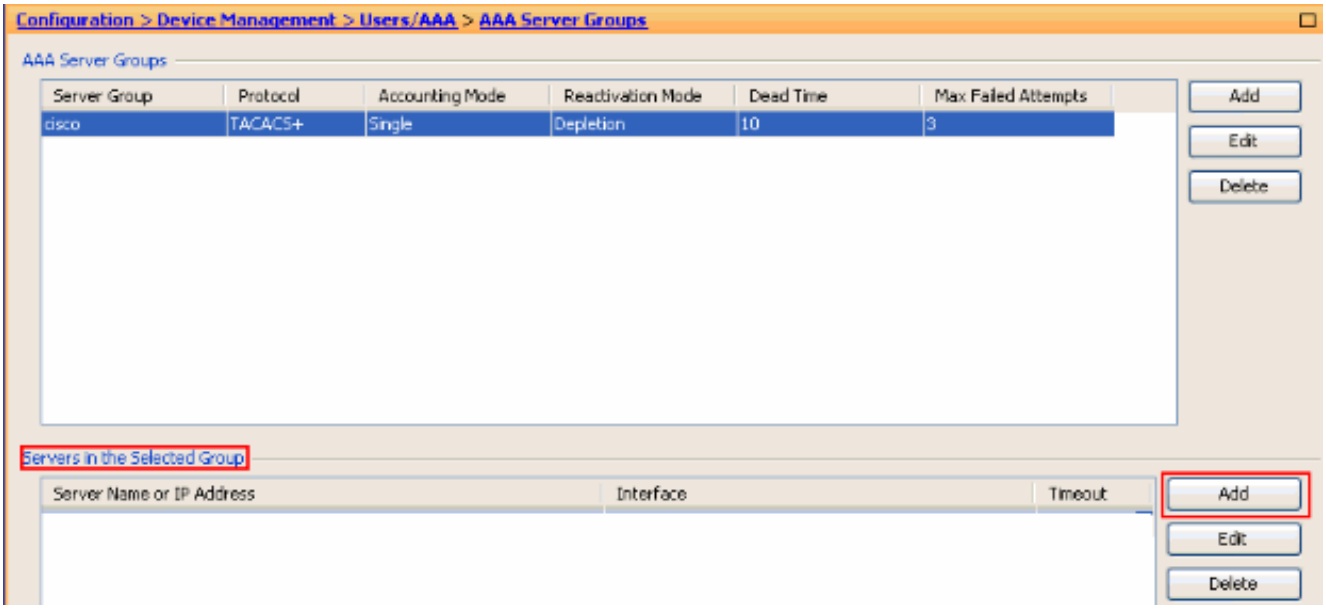


2. Proporcione a los detalles del **Grupo de servidores AAA** en la ventana de **Grupo de servidores AAA del agregar** como se muestra. El protocolo usado es **TACACS+** y el grupo de servidores creado es

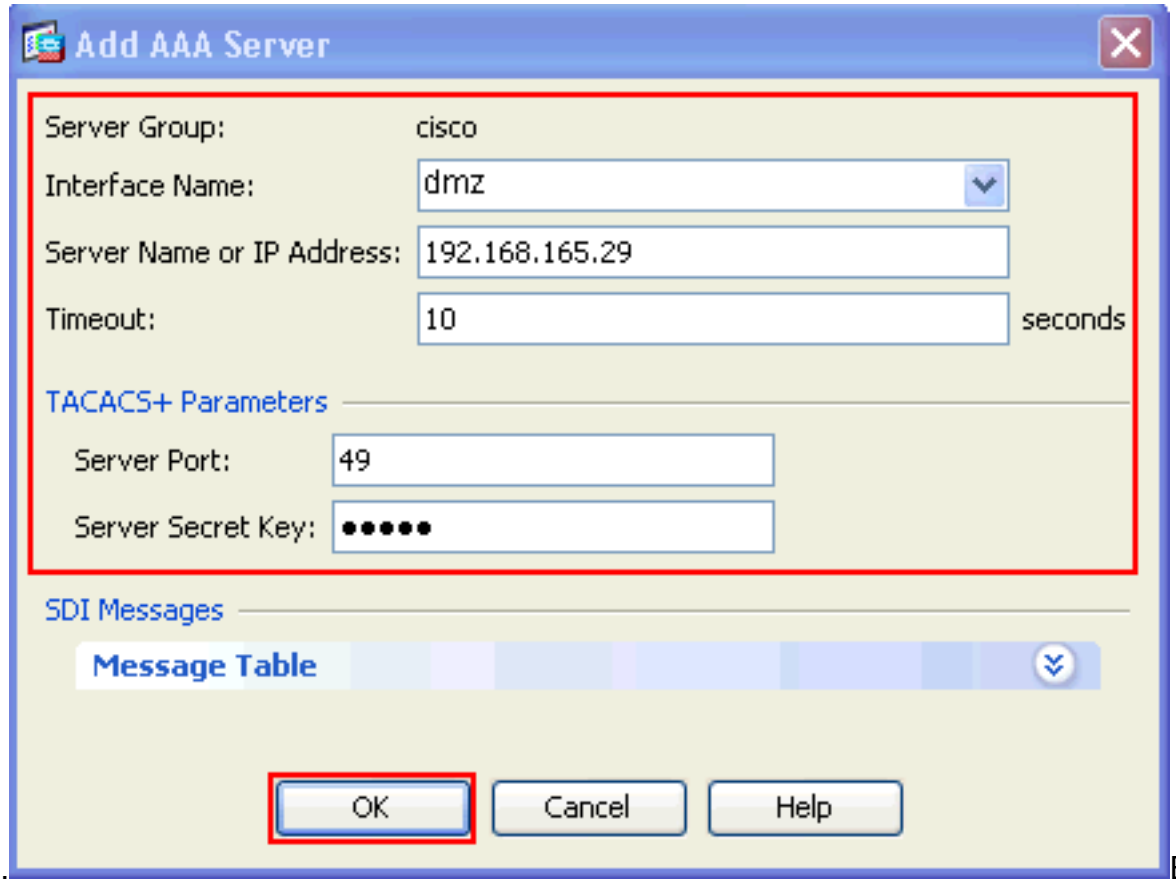


Cisco. Haga clic en OK.

3. Elija la **configuración > la Administración de dispositivos > a los grupos de servidores Users/AAA >AAA** y el tecleo **agrega** bajo los **servidores en el grupo seleccionado** para agregar al servidor de AAA.

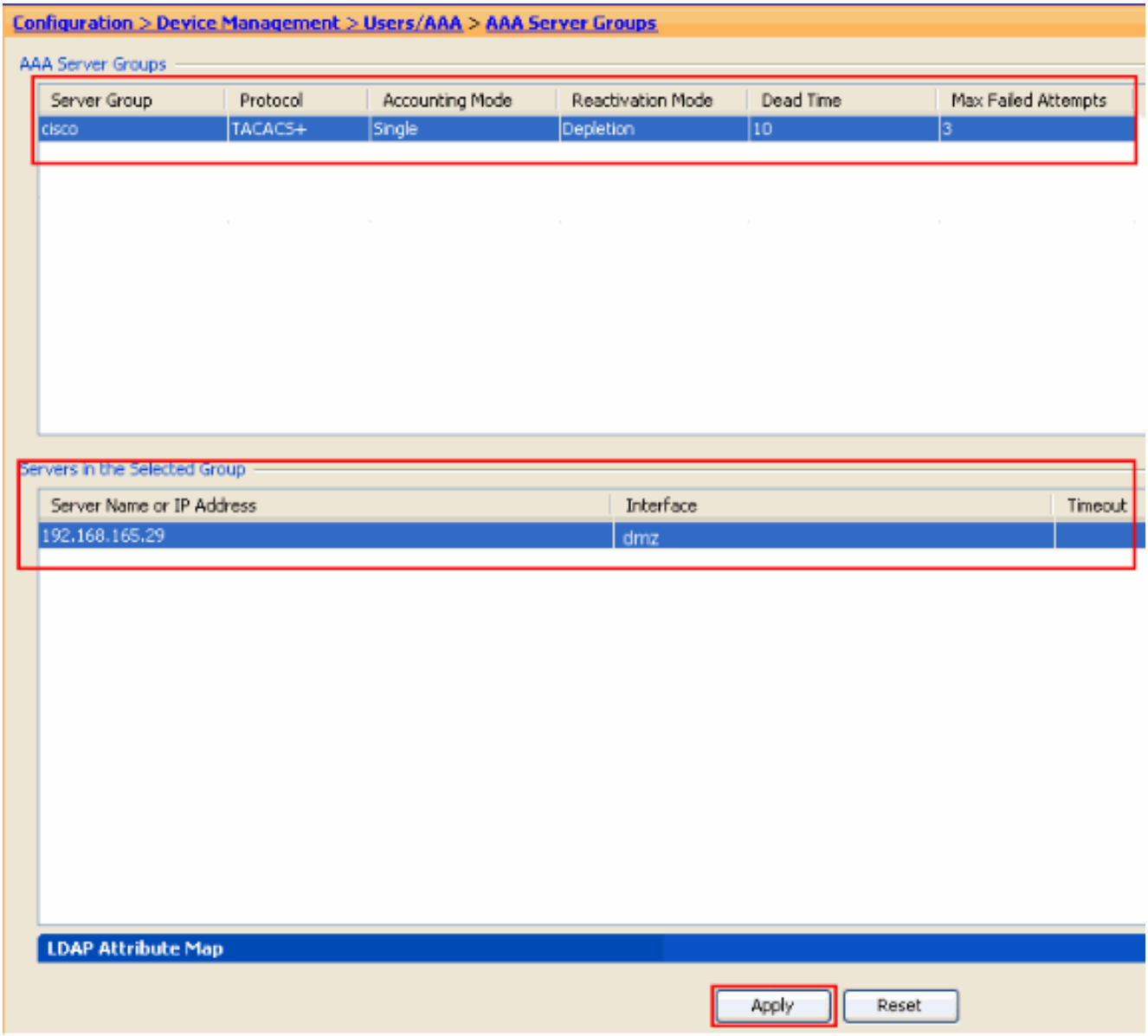


4. Proporcione a los detalles del **servidor de AAA** en la ventana del **servidor de AAA del agregar** como se muestra. El grupo de servidores usado es

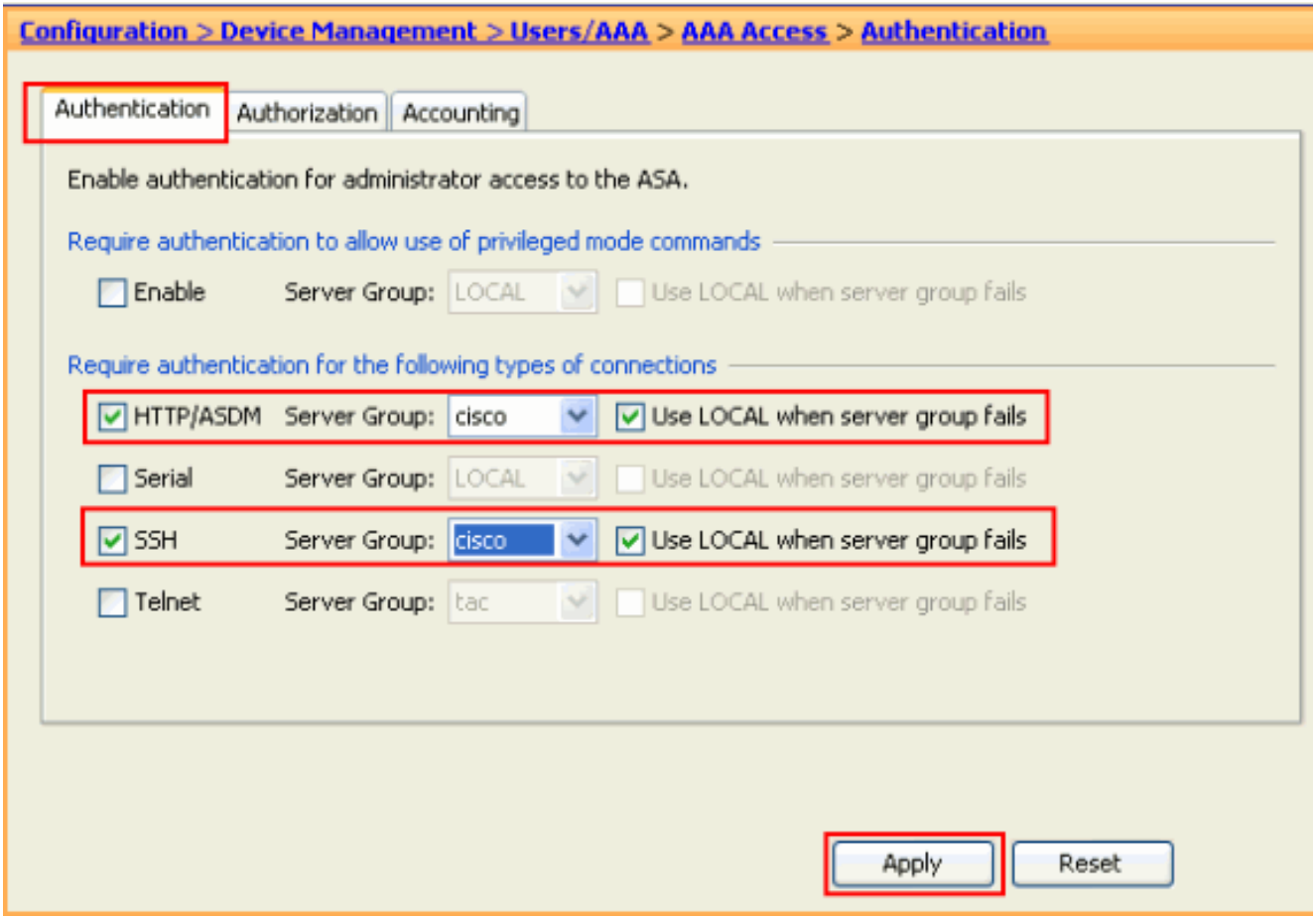


Cisco.El Haga Click en OK, entonces hace clic **se aplica**.Usted verá el **Grupo de servidores AAA** y al **servidor de AAA** configurados en el ASA.

5. Haga clic en Apply
   (Aplicar).



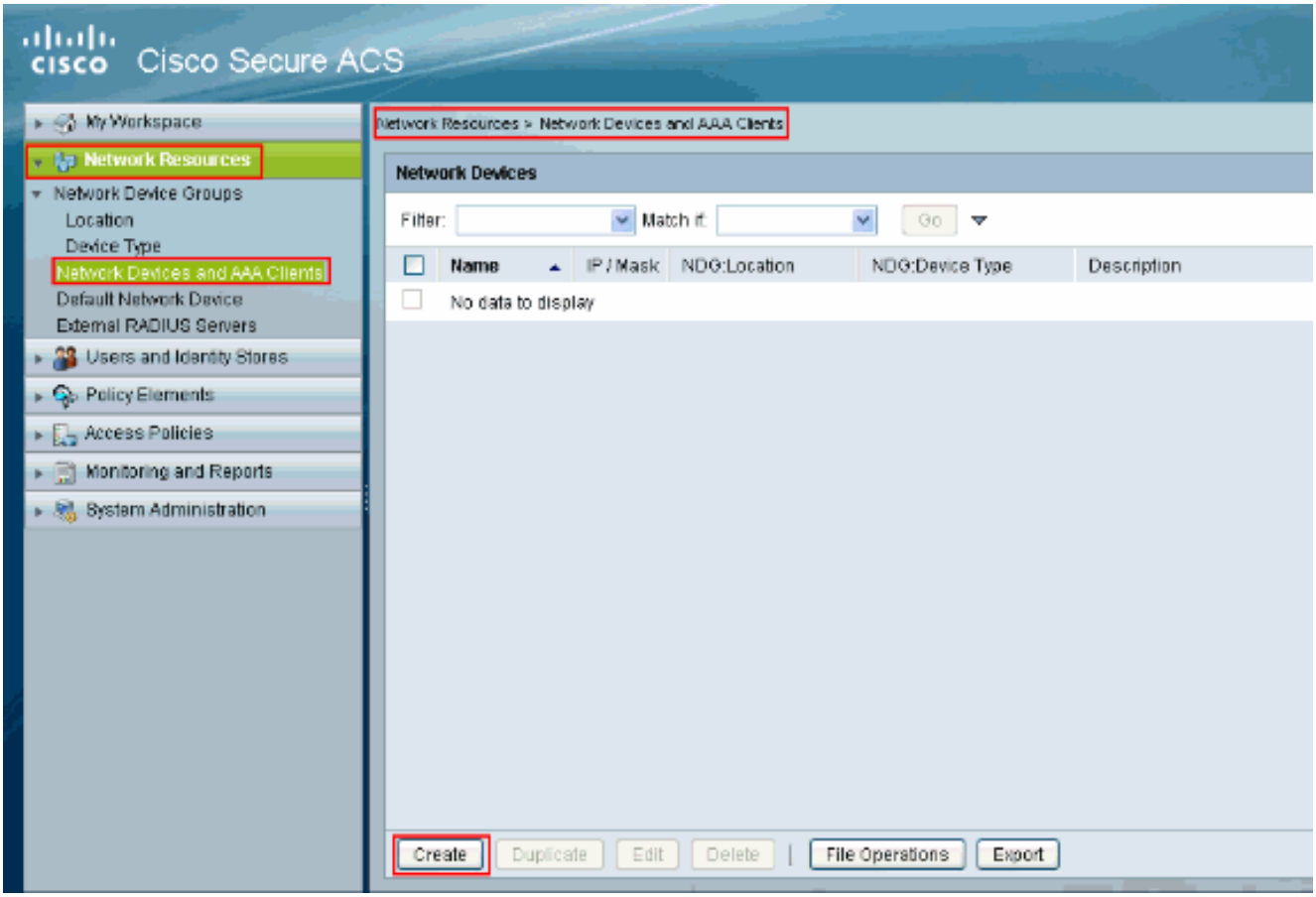
6. Elija la **configuración > la Administración de dispositivos > el acceso > la autenticación Users/AAA >AAA** y haga clic las casillas de verificación al lado de **HTTP/ASDM** y de **SSH**. Entonces, elija **Cisco** como el grupo de servidores y el tecleo **se aplica**.



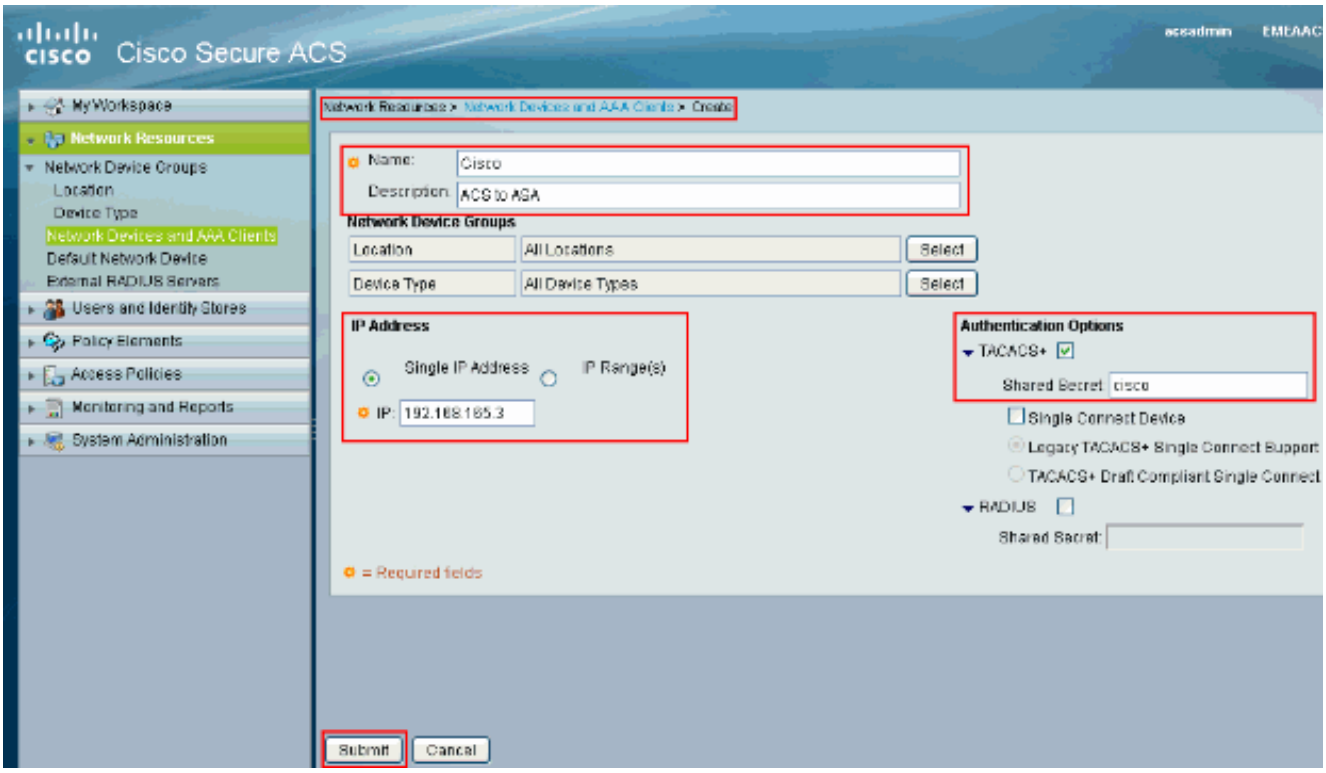
Configuración ACS como servidor TACACS

Complete este procedimiento para configurar el ACS como servidor TACACS:

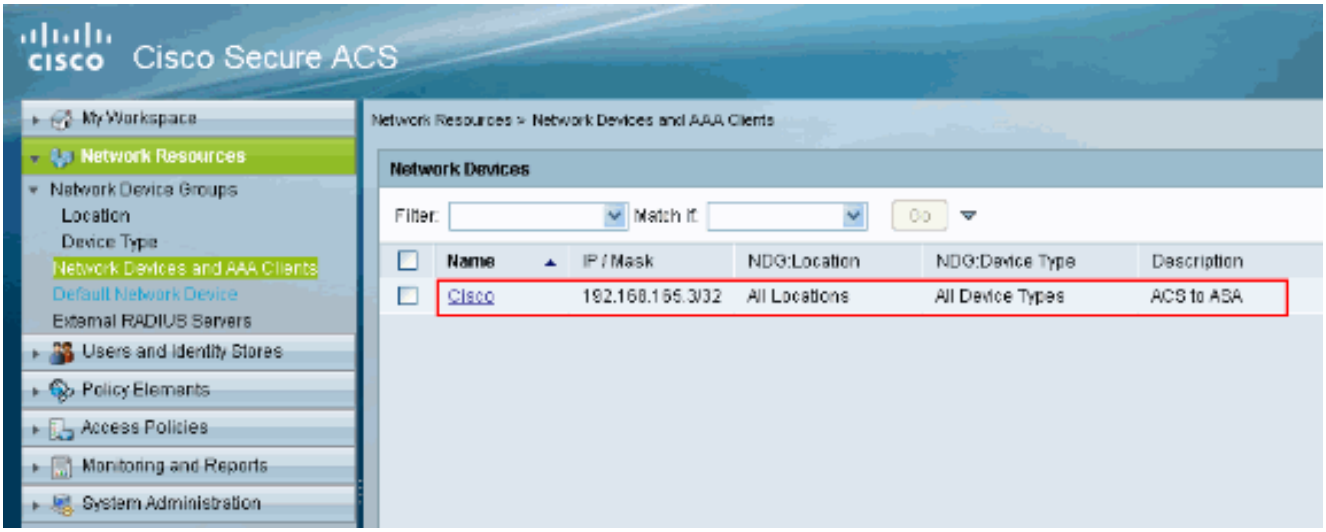
1. Elija los **recursos de red > los dispositivos de red y los clientes AAA** y el tecleo **crean** para agregar el ASA al servidor
   ACS.



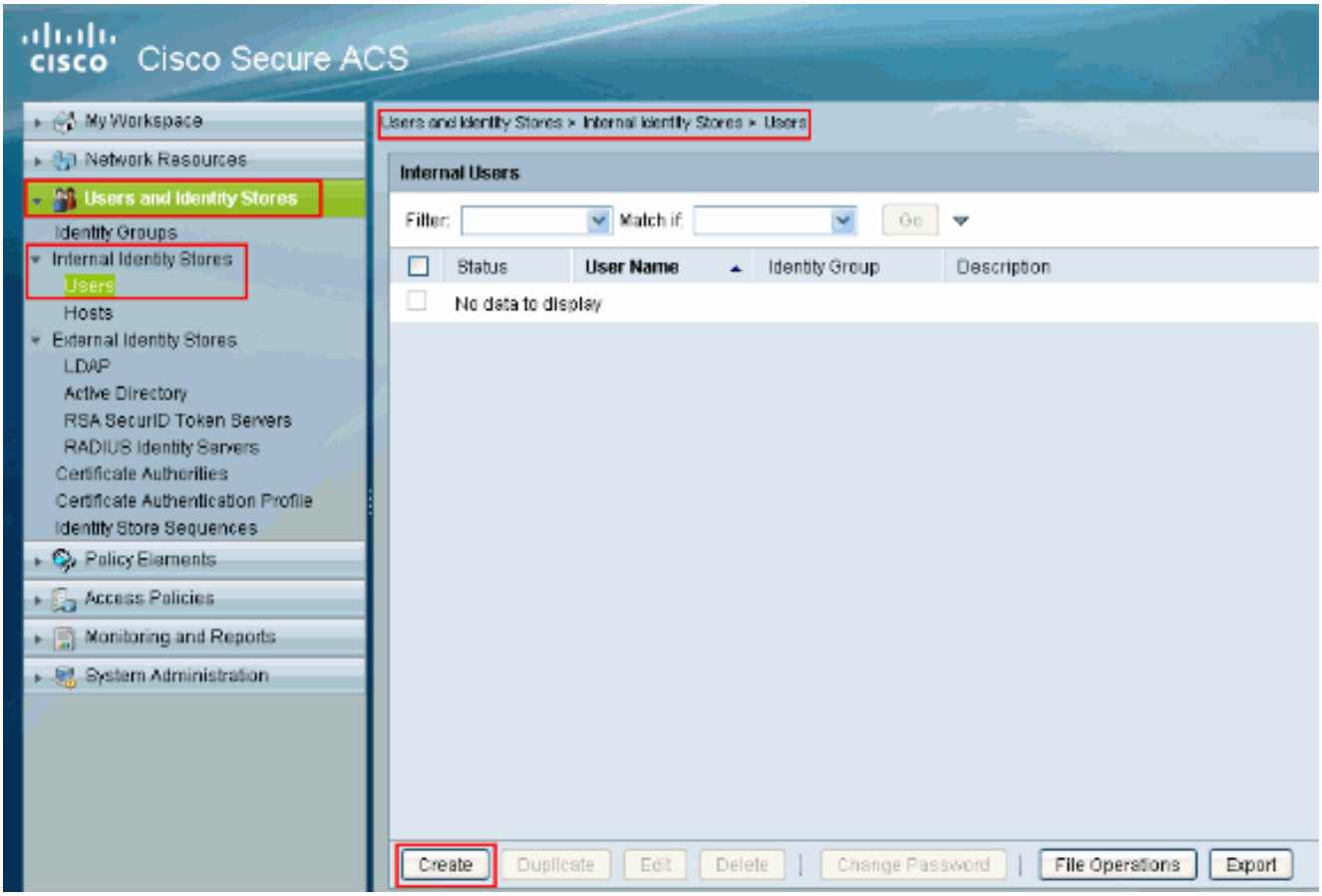
2. Proporcione la Información requerida sobre el **cliente** (ASA es el cliente aquí) y el tecleo **somete**. Este enablesthe ASA a conseguir agregó al servidor ACS. Los detalles incluyen la **dirección IP del** ASA y de los detalles del **servidor TACACS**.



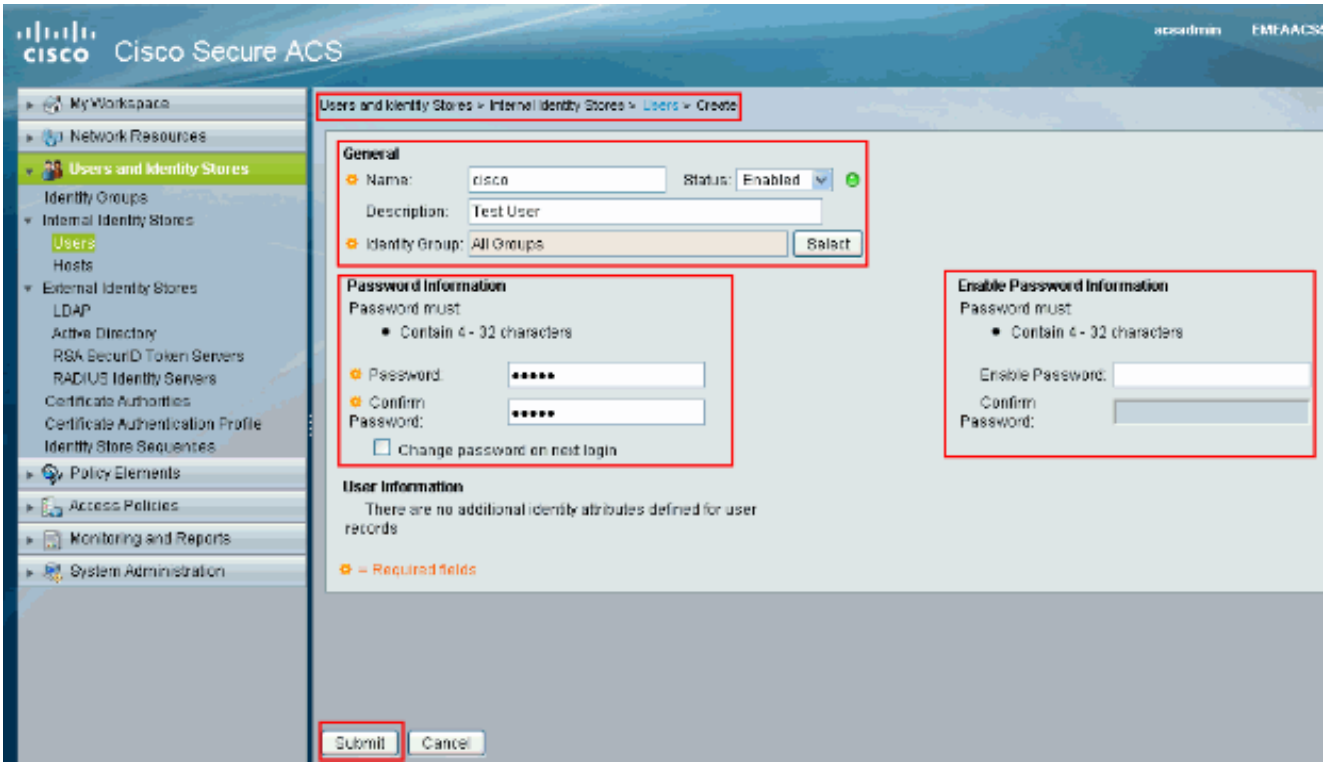
Usted verá al cliente **Cisco** que es agregado al servidor ACS.



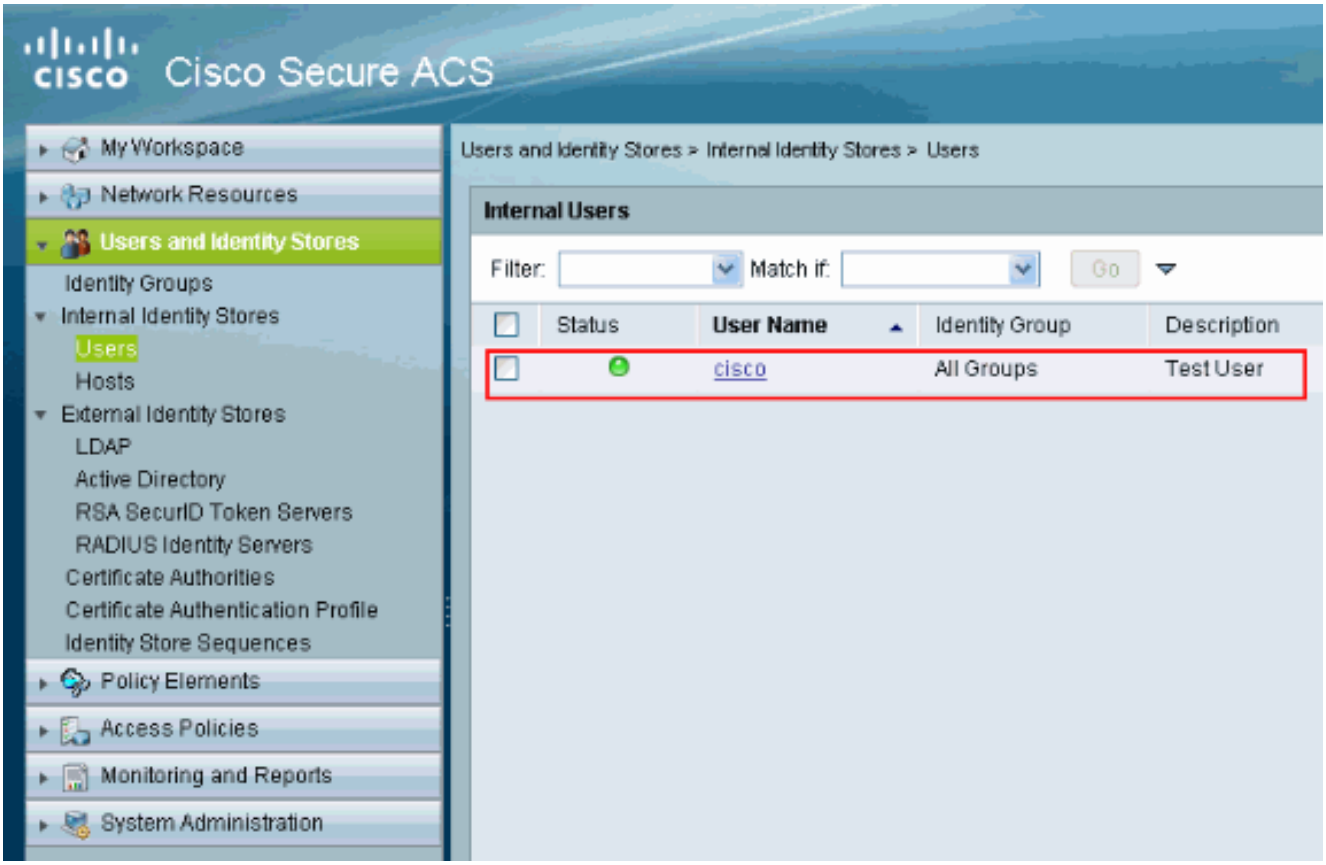
3. Elija a los **usuarios y la identidad salva > los almacenes internos de la identidad > Users** y el tecleo **crea** para crear a un usuario nuevo.



4. Proporcione la información del **nombre, de la contraseña, y de contraseña habilitada**. **La contraseña habilitada** es **opcional**. Cuando usted acaba, el tecleo **somete**.



Usted verá al usuario **Cisco** que es agregado al servidor ACS.

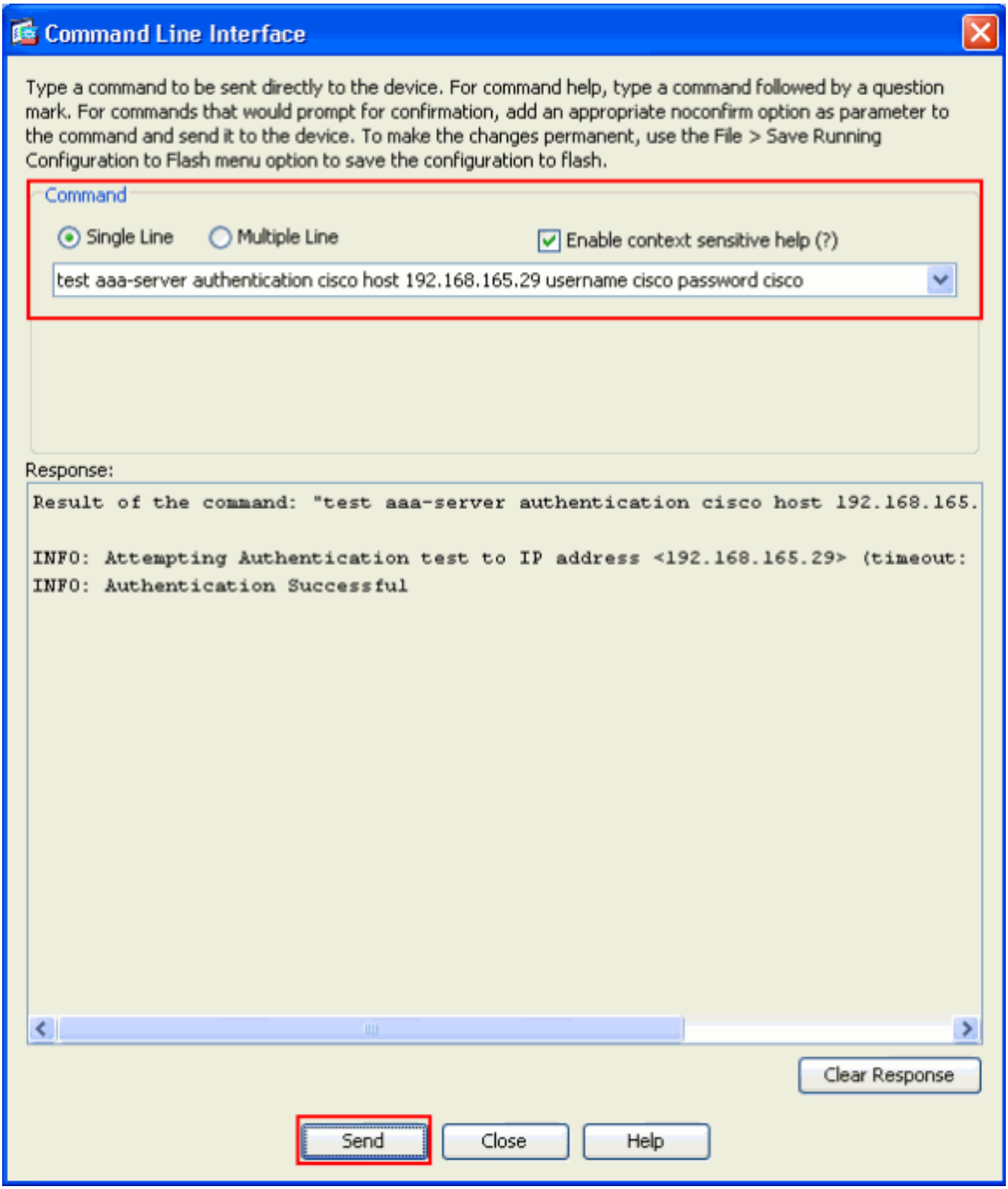


Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Utilice el **comando password cisco** más thetest del **nombre de usuario cisco de 192.168.165.29 del host de Cisco de la autenticación del AAA-servidor** de marcar si la configuración trabaja correctamente. Esta imagen muestra que la autenticación es acertada y al servidor ACS ha

autenticado al usuario que conectaba con el ASA.



La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Troubleshooting

Error: AAA que marca el servidor x.x.x.x TACACS+ en los tacacs del Grupo de

servidores AAA según lo FALLADO

Este mensaje significa que Cisco ASA perdió la Conectividad con el servidor x.x.x.x. Aseegurese le tener una Conectividad válida en el TCP 49 al servidor x.x.x.x del ASA. Usted puede también aumentar el descanso en el ASA para el servidor TACACS+ a partir del 5 al número deseado de segundos en caso de que haya una latencia de red. El ASA no enviaría un pedido de autenticación al servidor defectuoso x.x.x.x. Sin embargo, utilizará el servidor siguiente en los tacacs del Grupo de servidores AAA.

Información Relacionada

- Página de Soporte de Cisco ASA 5500 Series Adaptive Security Appliances
- Referencias de comandos del Dispositivos de seguridad adaptable Cisco ASA de la serie 5500
- Cisco Adaptive Security Device Manager
- Página de Soporte de IPSec Negotiation/IKE Protocols
- Cisco Secure Access Control Server para Windows
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems