

ASA 8.3: TACACS Authentication using ACS 5.X

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[Configure](#)

[Network Diagram](#)

[Configure the ASA for Authentication from ACS Server using CLI](#)

[Configure ASA for Authentication from ACS Server using ASDM](#)

[Configure ACS as a TACACS Server](#)

[Verify](#)

[Troubleshoot](#)

[Error: AAA Marking TACACS+ server x.x.x.x in aaa-server group tacacs as FAILED](#)

[Related Information](#)

[Introduction](#)

This document provides information on how to configure the security appliance to authenticate users for network access.

[Prerequisites](#)

[Requirements](#)

This document assumes that the Adaptive Security Appliance (ASA) is fully operational and configured to allow the Cisco Adaptive Security Device Manager (ASDM) or CLI to make configuration changes.

Note: Refer to [Allowing HTTPS Access for ASDM](#) for more information on how to allow the device to be remotely configured by the ASDM.

[Components Used](#)

The information in this document is based on these software and hardware versions:

- Cisco Adaptive Security Appliance Software Version 8.3 and later
- Cisco Adaptive Security Device Manager Version 6.3 and later

- Cisco Secure Access Control Server 5.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

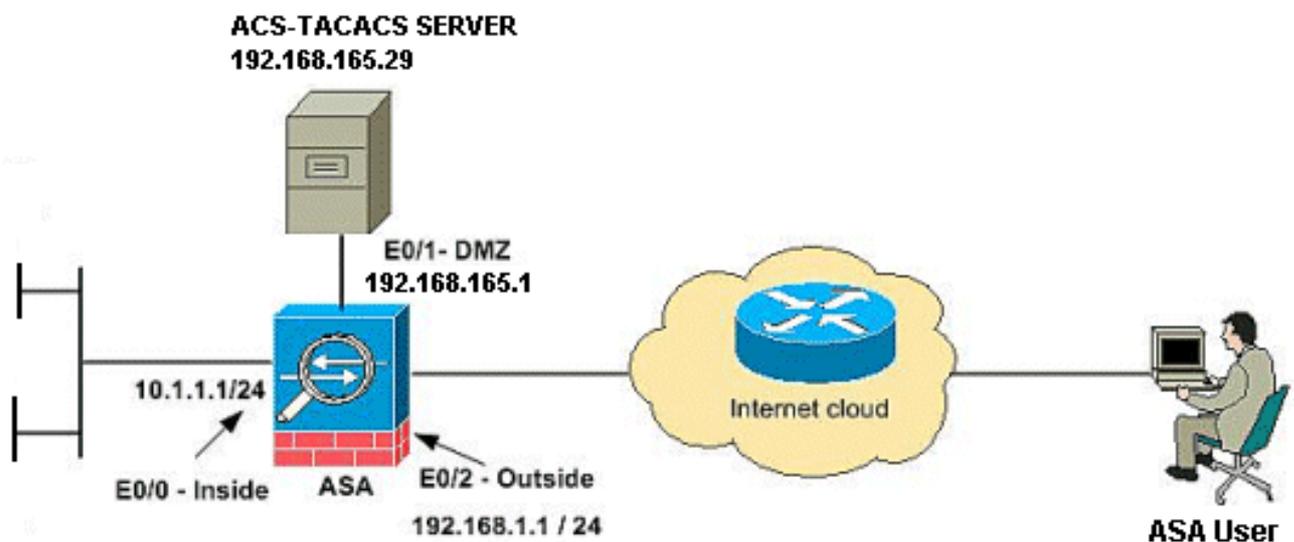
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the [Command Lookup Tool](#) ([registered](#) customers only) in order to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which were used in a lab environment.

Configure the ASA for Authentication from ACS Server using CLI

Perform these configurations for the ASA to authenticate from the ACS server:

```
!--- 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
```

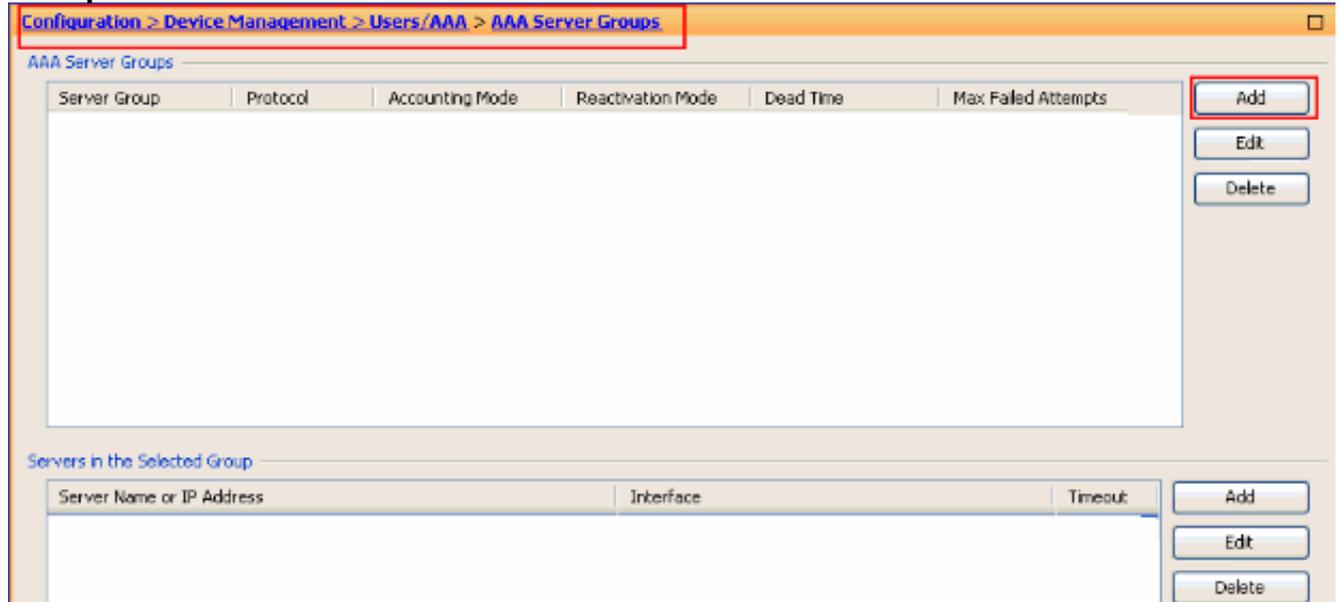
Note: Create a local user on the ASA using the [username cisco password cisco privilege 15](#) command to access the ASDM with local authentication when the ACS is not available.

[Configure ASA for Authentication from ACS Server using ASDM](#)

ASDM Procedure

Complete these steps in order to configure the ASA for authentication from the ACS server:

1. Choose **Configuration > Device Management > Users/AAA > AAA Server Groups > Add** in order to create an **AAA Server Group**.



2. Provide the **AAA Server Group** details in the **Add AAA Server Group** window as shown. The protocol used is **TACACS+** and the server group created is

Server Group:

Protocol:

Accounting Mode: Simultaneous Single

Reactivation Mode: Depletion Timed

Dead Time: minutes

Max Failed Attempts:

cisco. Click **OK**.

- Choose **Configuration > Device Management > Users/AAA > AAA Server Groups** and click **Add** under **Servers in the Selected Group** in order to add the AAA server.

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
cisco	TACACS+	Single	Depletion	10	3

Servers in the Selected Group

Server Name or IP Address	Interface	Timeout

- Provide the **AAA Server** details in the **Add AAA Server** window as shown. The server group used is

Add AAA Server

Server Group: cisco

Interface Name: dmz

Server Name or IP Address: 192.168.165.29

Timeout: 10 seconds

TACACS+ Parameters

Server Port: 49

Server Secret Key: ●●●●●●

SDI Messages

Message Table

OK Cancel Help

cisco.

Click

click **OK**, then click **Apply**. You will see the **AAA Server Group** and the **AAA Server** configured on the ASA.

5. Click **Apply**.

Configuration > Device Management > Users/AAA > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
cisco	TACACS+	Single	Depletion	10	3

Servers in the Selected Group

Server Name or IP Address	Interface	Timeout
192.168.165.29	dmz	

LDAP Attribute Map

Apply Reset

6. Choose **Configuration > Device Management > Users/AAA > AAA Access > Authentication** and click the check boxes next to **HTTP/ASDM** and **SSH**. Then, choose **cisco** as the server group and click **Apply**.

[Configuration](#) > [Device Management](#) > [Users/AAA](#) > [AAA Access](#) > [Authentication](#)

Authentication Authorization Accounting

Enable authentication for administrator access to the ASA.

Require authentication to allow use of privileged mode commands _____

Enable Server Group: LOCAL Use LOCAL when server group fails

Require authentication for the following types of connections _____

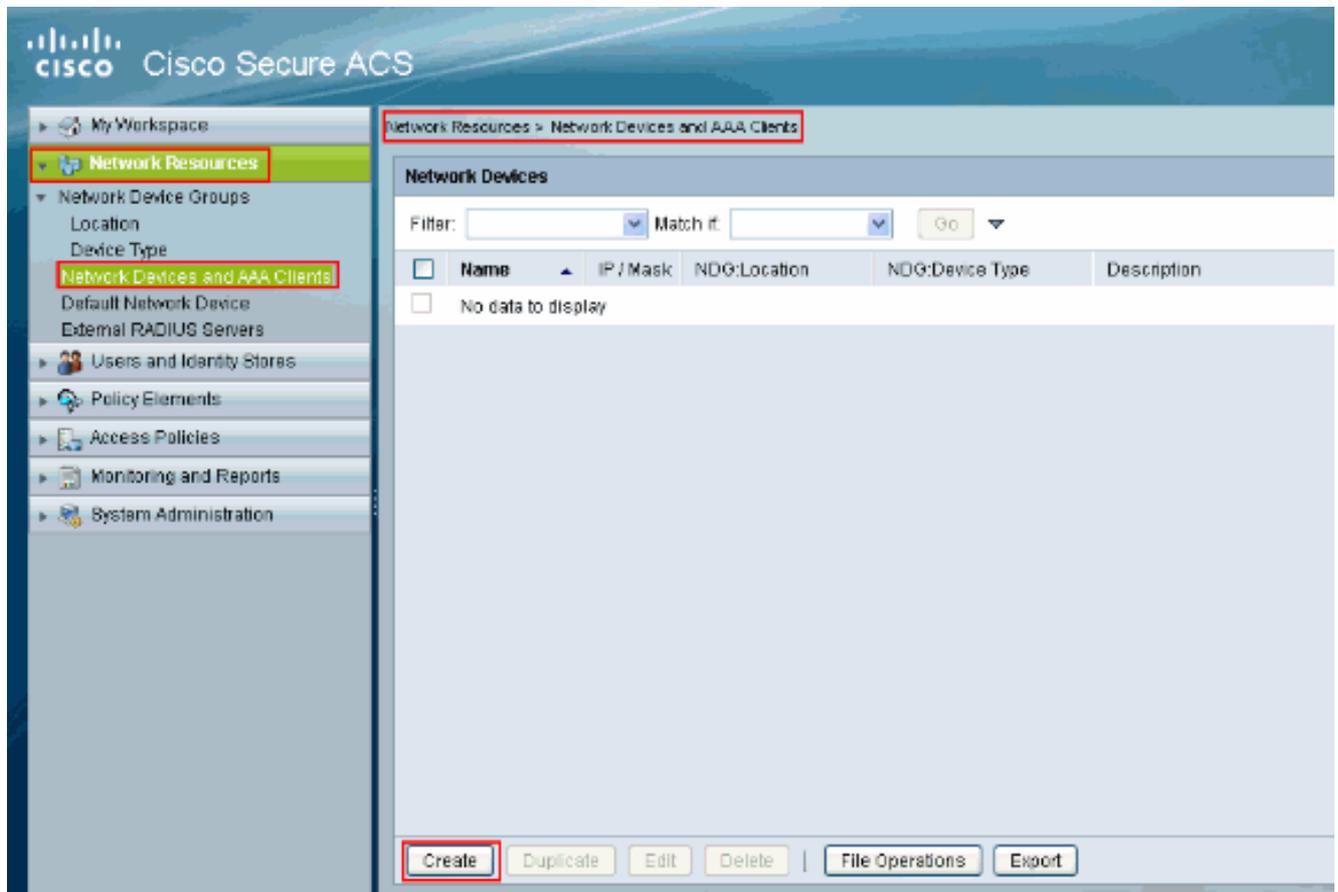
<input checked="" type="checkbox"/> HTTP/ASDM	Server Group: cisco	<input checked="" type="checkbox"/> Use LOCAL when server group fails
<input type="checkbox"/> Serial	Server Group: LOCAL	<input type="checkbox"/> Use LOCAL when server group fails
<input checked="" type="checkbox"/> SSH	Server Group: cisco	<input checked="" type="checkbox"/> Use LOCAL when server group fails
<input type="checkbox"/> Telnet	Server Group: tac	<input type="checkbox"/> Use LOCAL when server group fails

Apply Reset

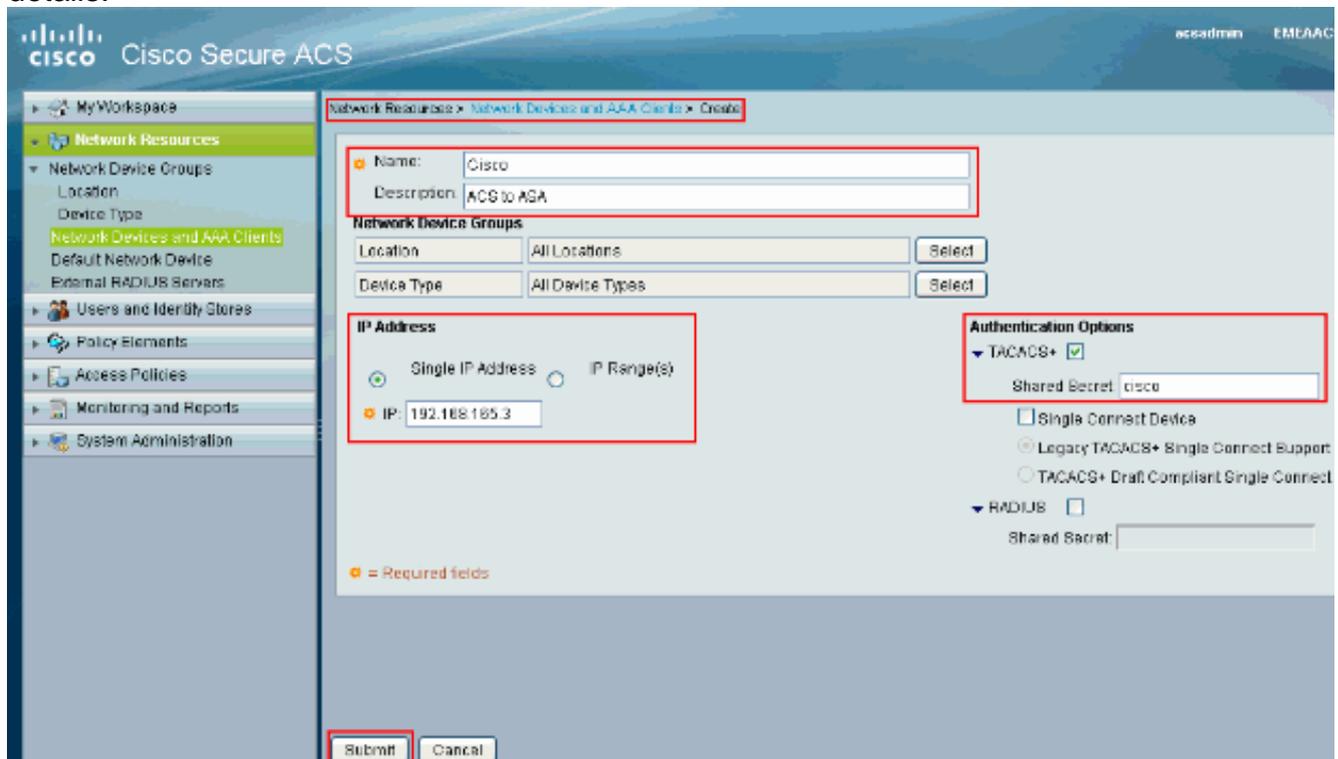
[Configure ACS as a TACACS Server](#)

Complete this procedure in order to configure the ACS as a TACACS server:

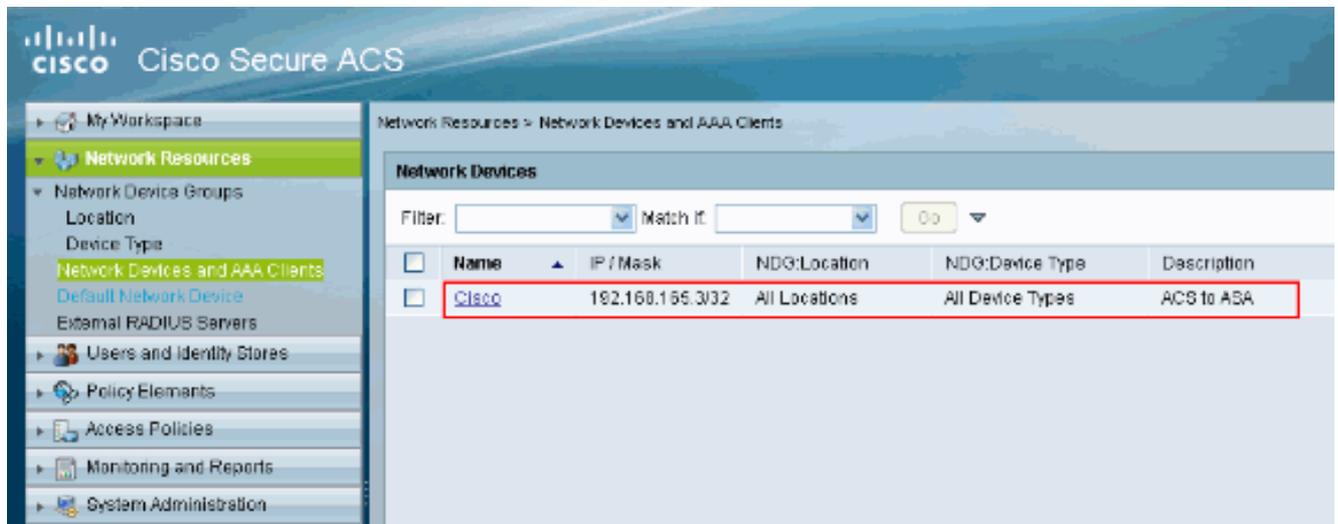
1. Choose **Network Resources > Network Devices and AAA Clients** and click **Create** in order to add the ASA to the ACS server.



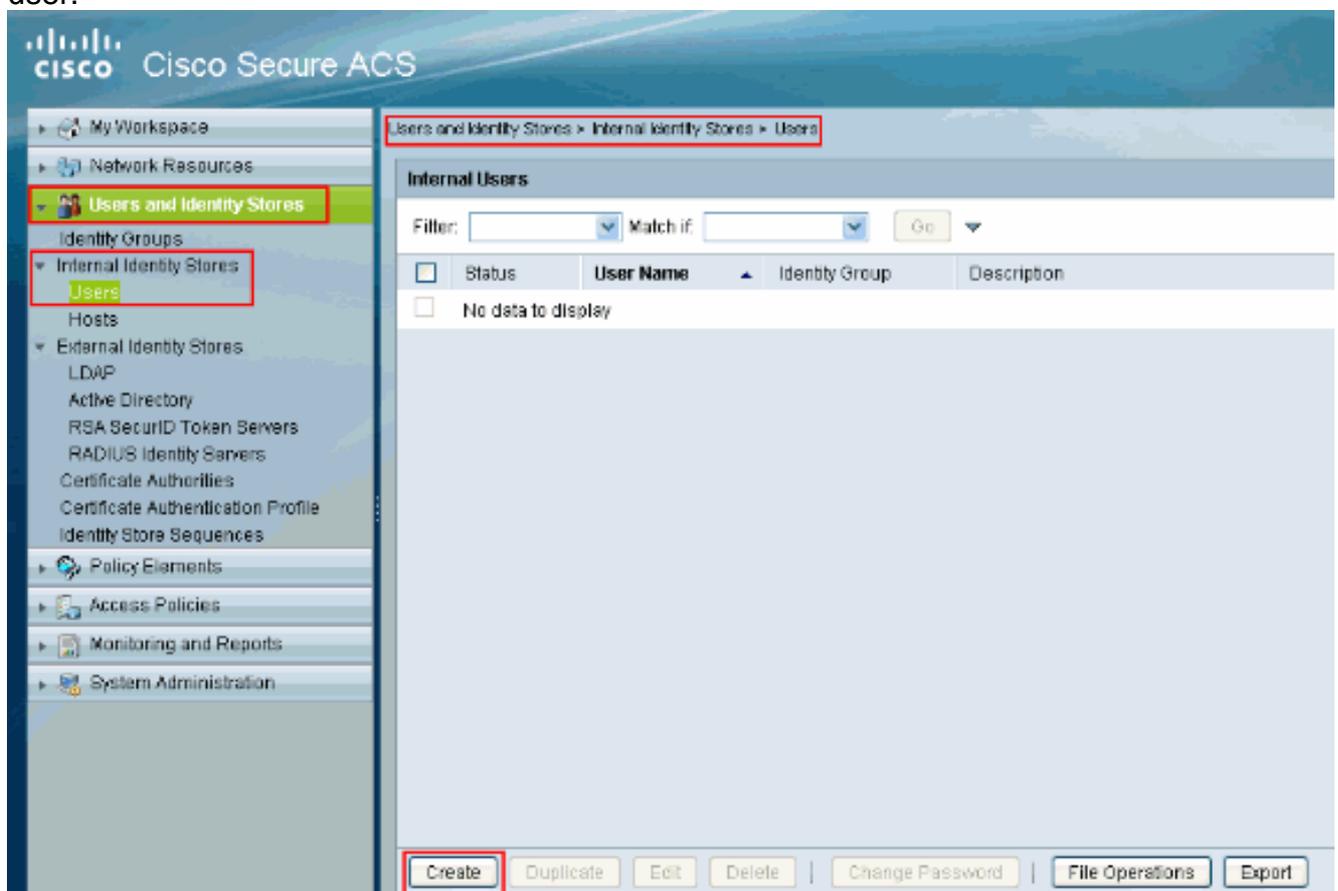
2. Provide the required information about the **client** (ASA is the client here) and click **Submit**. This enables the ASA to get added to the ACS server. The details include the **IP Address** of the ASA and the **TACACS server** details.



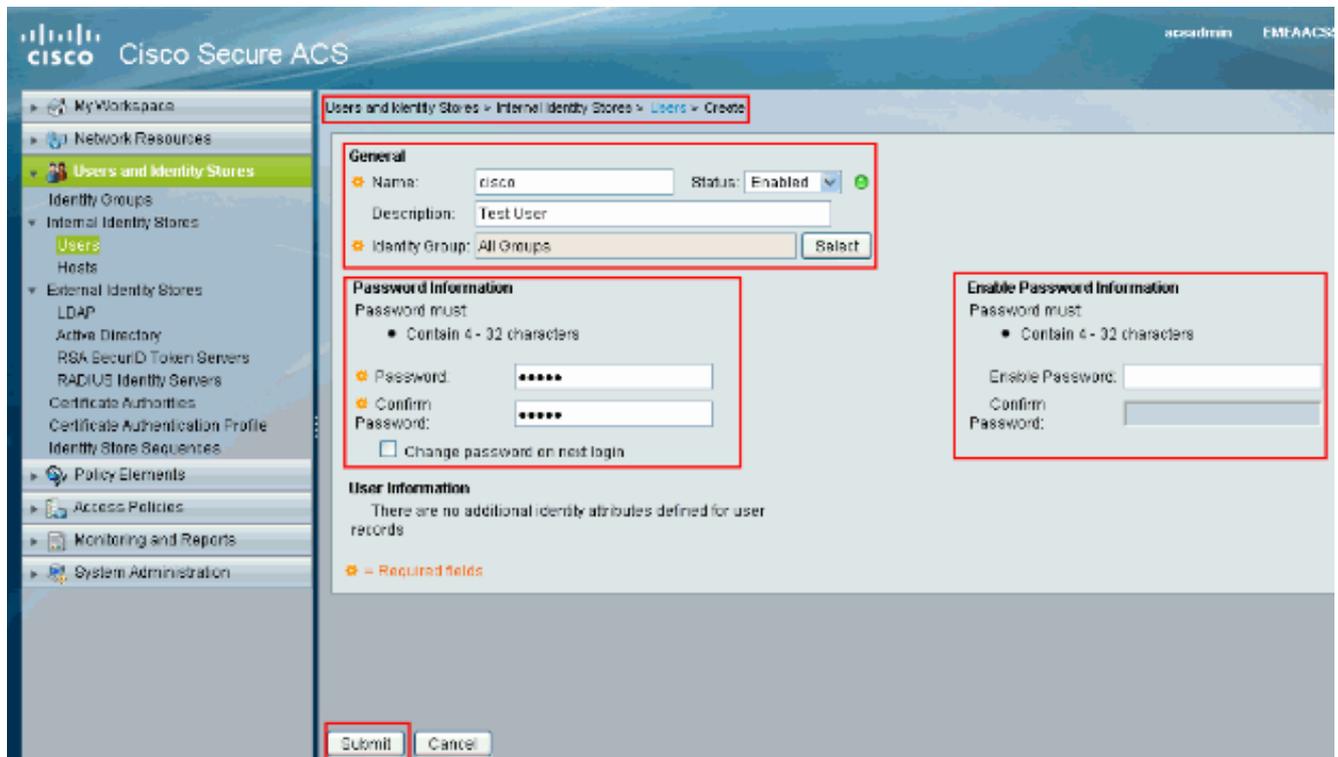
You will see the client **Cisco** being added to the ACS server.



3. Choose **Users and Identity stores > Internal Identity Stores > Users** and click **Create** in order to create a new user.



4. Provide the **Name, Password, and Enable Password** information. **Enable Password** is **optional**. When you finish, click **Submit**.



You will see the user **cisco** being added to the ACS server.

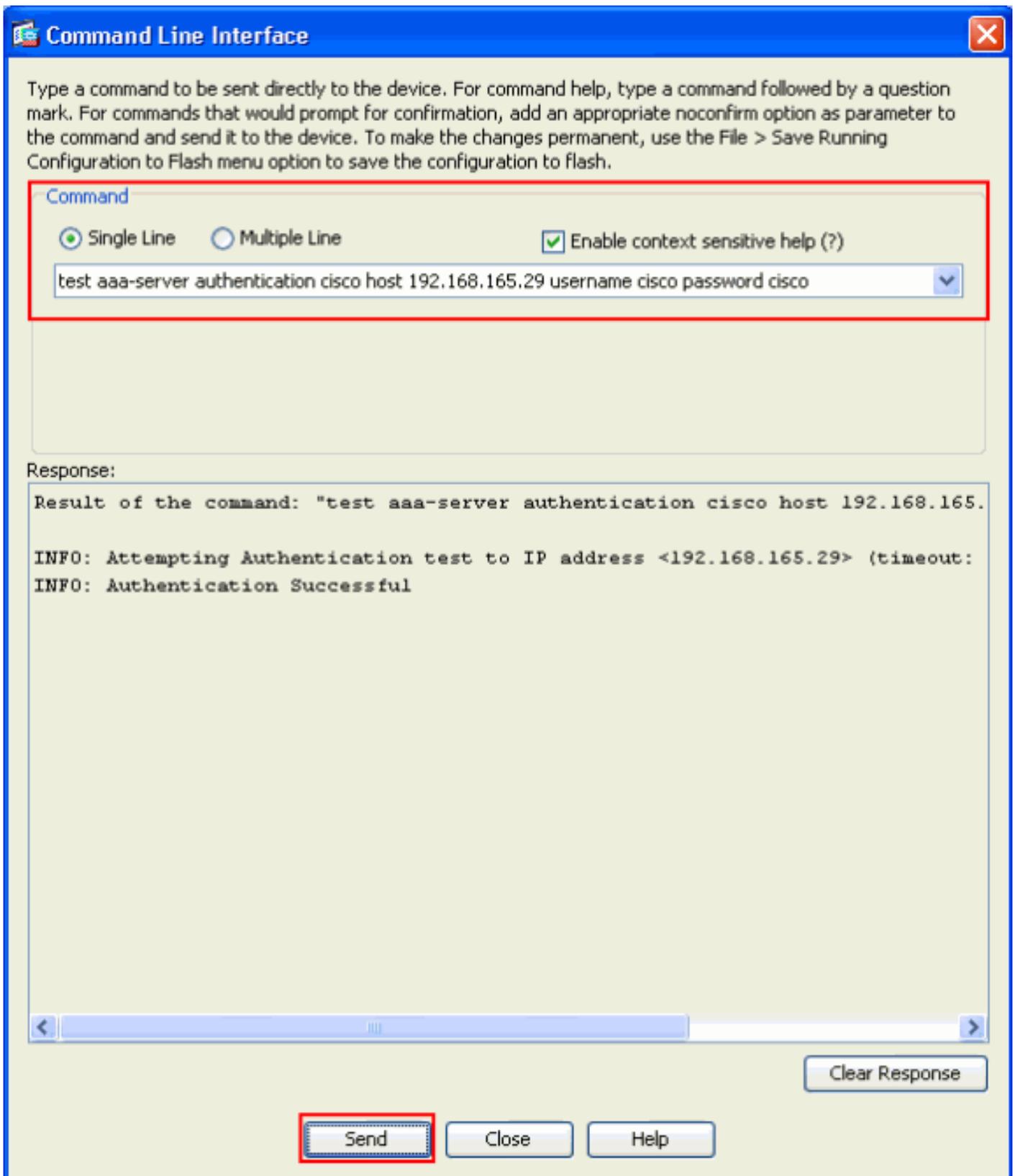


Verify

Use this section to confirm that your configuration works properly.

Use the **test aaa-server authentication cisco host 192.168.165.29 username cisco password cisco** command to check if the configuration works properly. This image shows that the authentication is successful and the user connecting to the ASA has been authenticated by the

ACS server.



The [Output Interpreter Tool](#) ([registered](#) customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

[Troubleshoot](#)

[Error: AAA Marking TACACS+ server x.x.x.x in aaa-server group tacacs as](#)

FAILED

This message means that Cisco ASA lost the connectivity with the x.x.x.x server. Make sure you have a valid connectivity on tcp 49 to server x.x.x.x from the ASA. You can also increase the timeout on the ASA for TACACS+ server from 5 to the desired number of seconds in case there is a network latency. The ASA would not send an authentication request to the FAILED server x.x.x.x. However, it will use the next server in the aaa-server group tacacs.

Related Information

- [**Cisco ASA 5500 Series Adaptive Security Appliances Support Page**](#)
- [**Cisco ASA 5500 Series Adaptive Security Appliances Command References**](#)
- [**Cisco Adaptive Security Device Manager**](#)
- [**IPsec Negotiation/IKE Protocols Support Page**](#)
- [**Cisco Secure Access Control Server for Windows**](#)
- [**Requests for Comments \(RFCs\)**](#) 
- [**Technical Support & Documentation - Cisco Systems**](#)