ASA 8. 3: Аутентификация TACACS с помощью ACS 5. X

Содержание

Введение

Этот документ предоставляет сведения о том, как настроить устройство безопасности для аутентификации пользователей для доступа к сети.

Предварительные условия

Требования

Этот документ предполагает, что Устройство адаптивной защиты (ASA) полностью в рабочем состоянии и настроено, чтобы позволить Cisco Adaptive Security Device Manager (ASDM) или CLI изменять конфигурацию.

Примечание: См. документ Разрешение HTTPS-доступа для ASDM для получения дополнительной информации о том, как позволить устройству быть удаленно настроенным ASDM.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Версия программного обеспечения 8.3 Устройства адаптивной защиты Cisco и позже
- Версия 6.3 Cisco Adaptive Security Device Manager и позже
- Сервер Cisco Secure Access Control Server 5. x

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

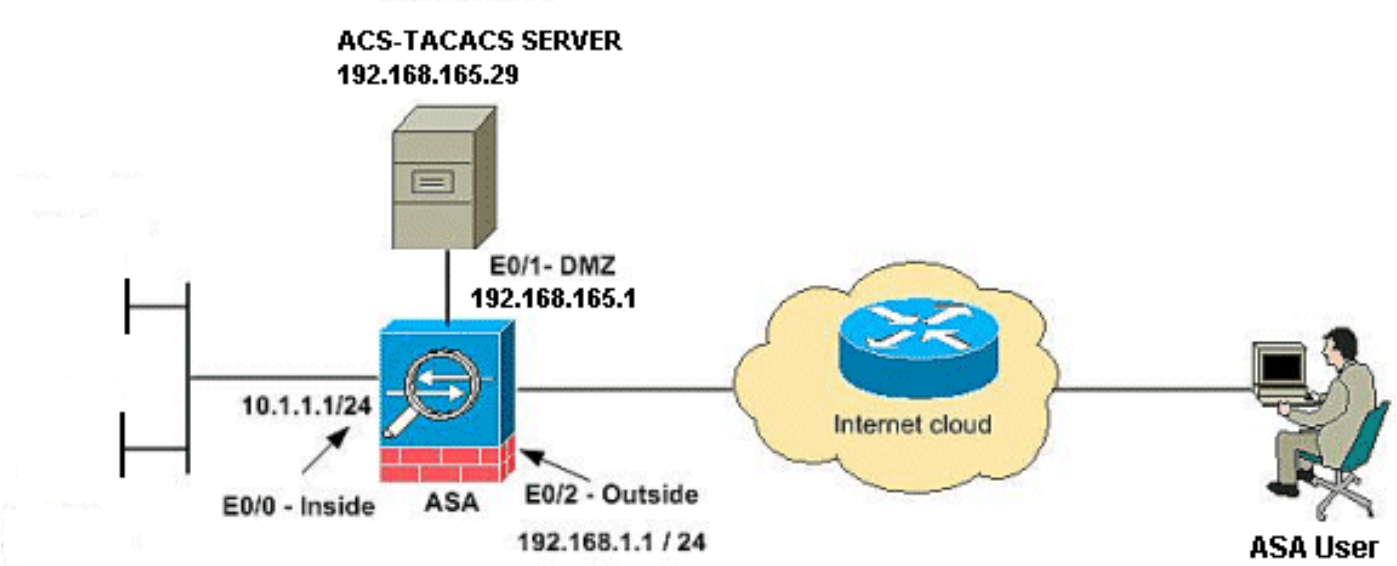
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:



Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, которые использовались в лабораторной среде.

Настройте ASA для Аутентификации от Сервера ACS с помощью CLI

Выполните эти конфигурации для ASA для аутентификации от сервера 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
```

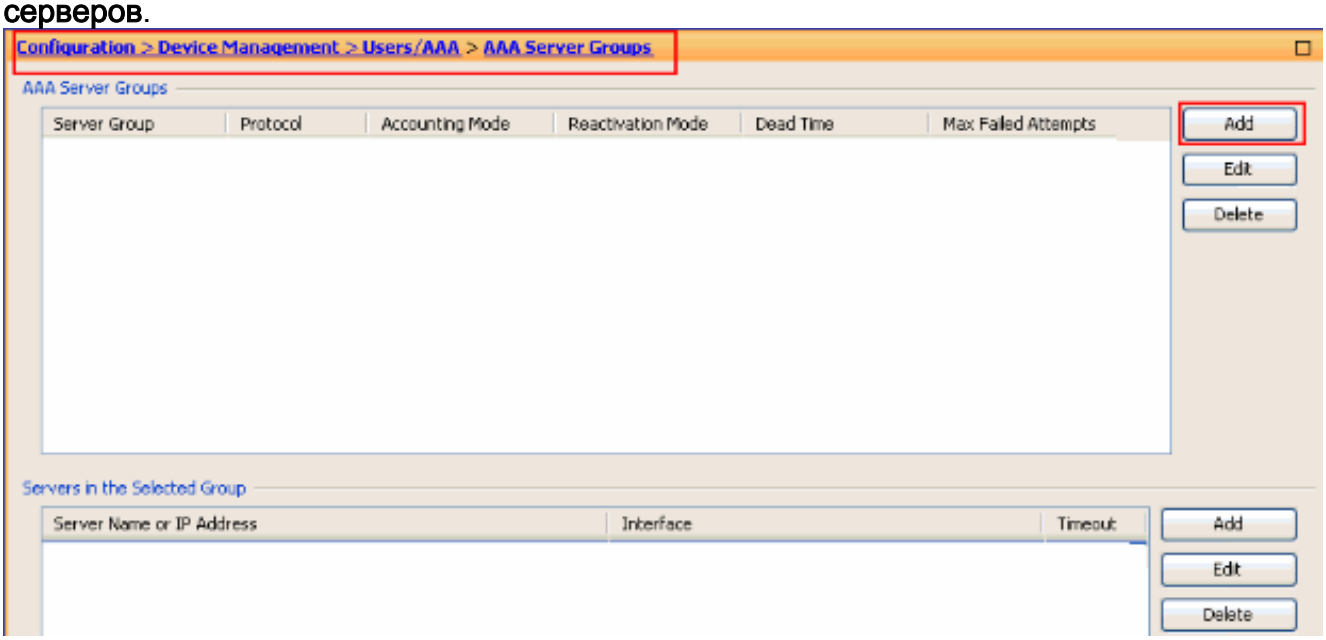
Примечание: Создайте локального пользователя на ASA с помощью **привилегии пароля cisco имени пользователя cisco 15** команд для доступа к ASDM с локальной проверкой подлинности, когда ACS не будет доступен.

Настройте ASA для Аутентификации от Сервера ACS с помощью ASDM

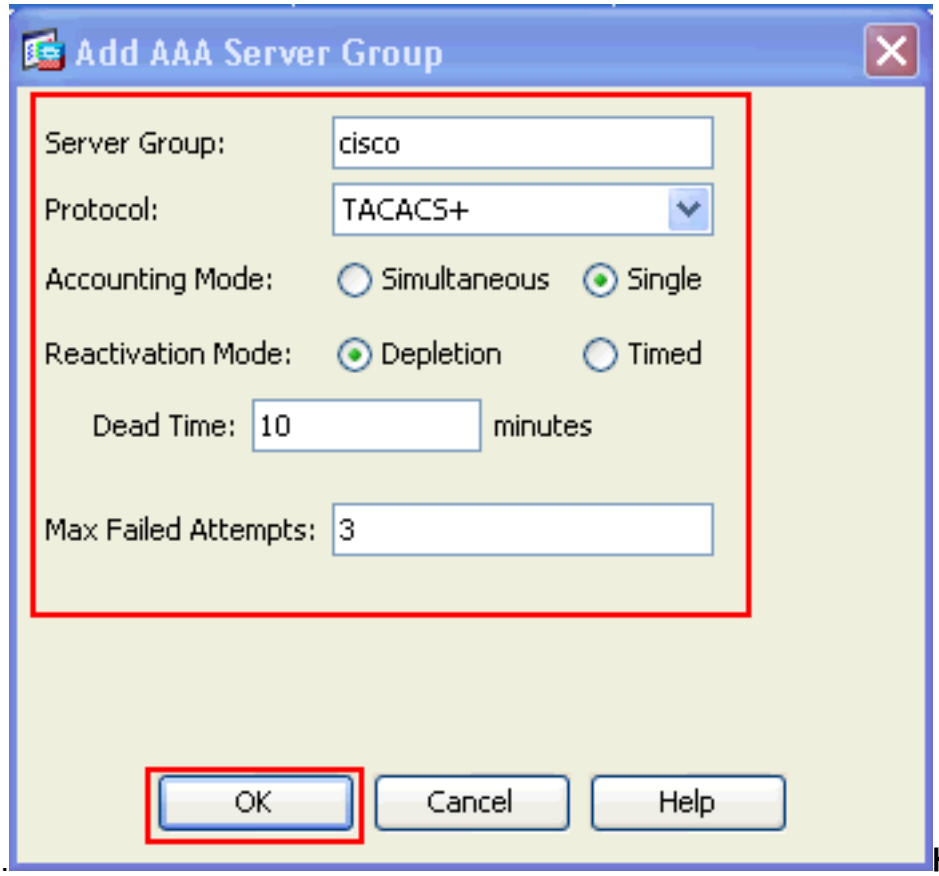
Порядок действий в диспетчере ASDM

Выполните эти шаги для настройки ASA для аутентификации от сервера ACS:

1. Выберите **Configuration>> Users Device Management / AAA>, Группы AAA-серверов> Добавляют** для создания **Группы AAA-серверов**.

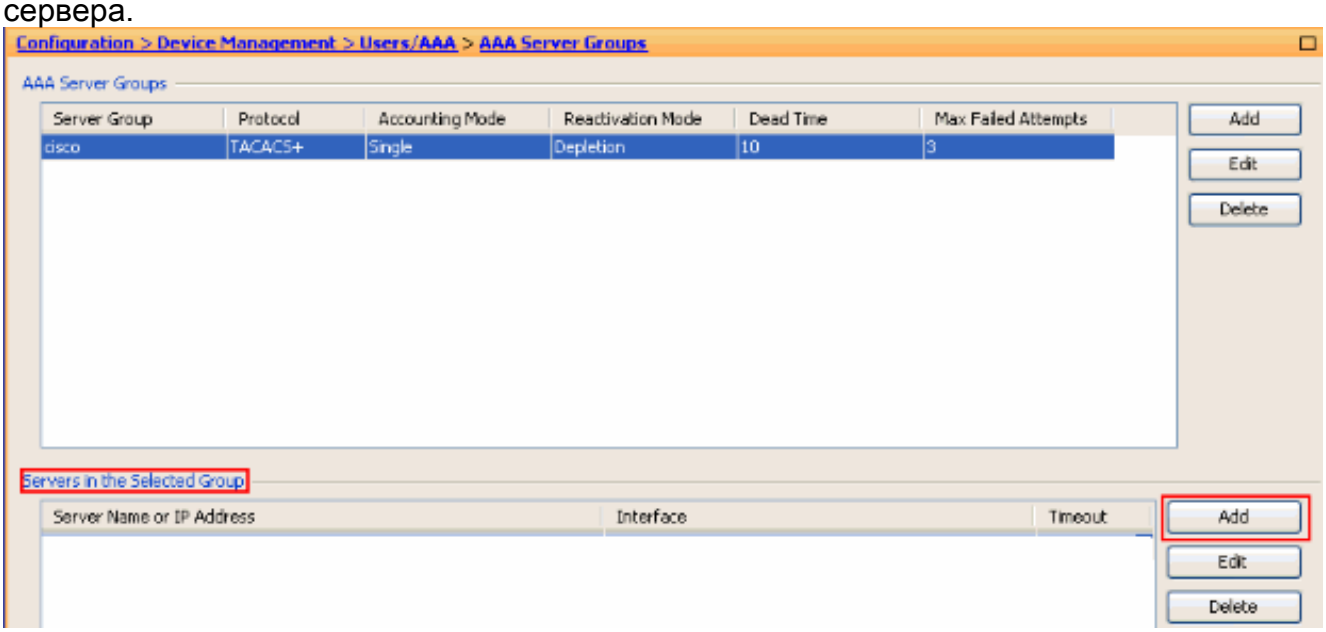


2. Предоставьте подробную информацию **Группы AAA-серверов** в окне **Add AAA Server Group** как показано. Используемый протокол является **TACACS +**, и созданная группа серверов является

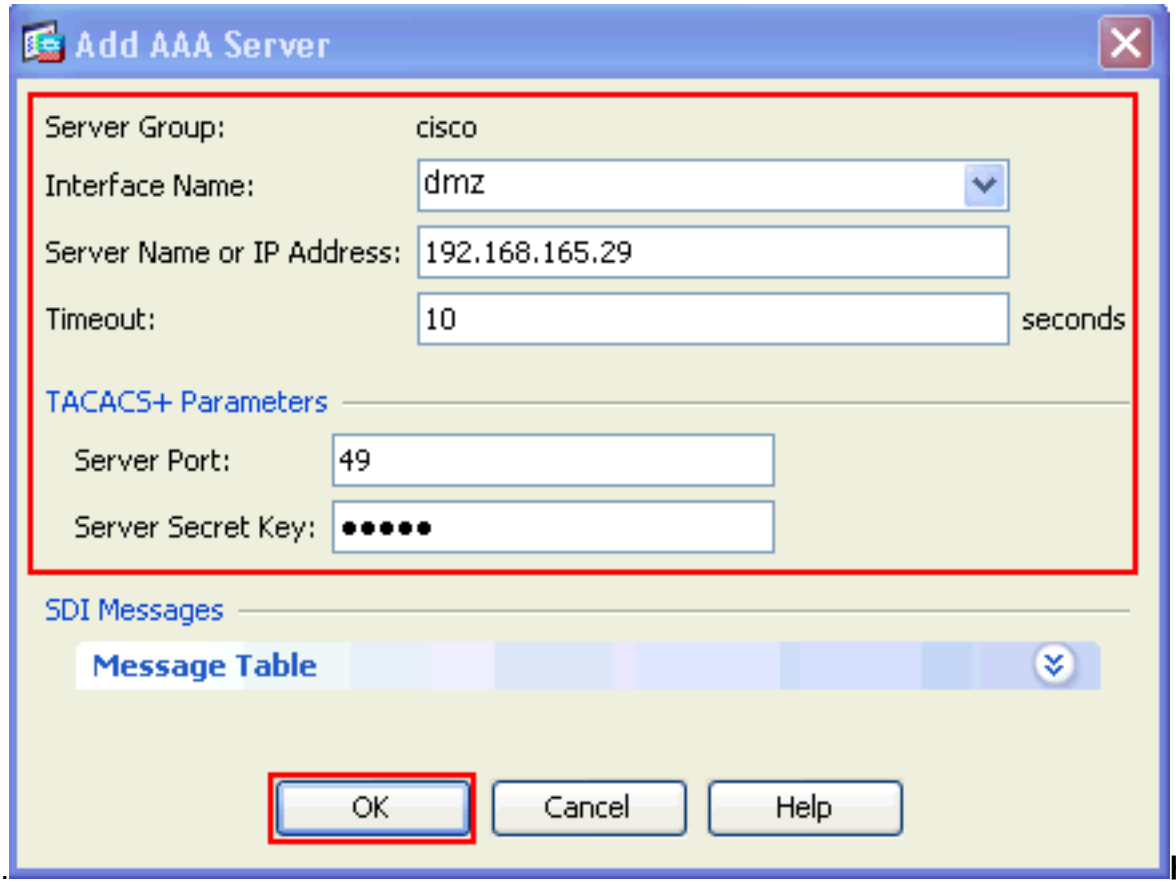


Cisco. **Нажмите кнопку OK.**

3. Выберите **Configuration>> Users Device Management / AAA> Группы AAA-серверов** и **нажмите Add** под **Серверами в Selected Group** для добавления AAA-сервера.

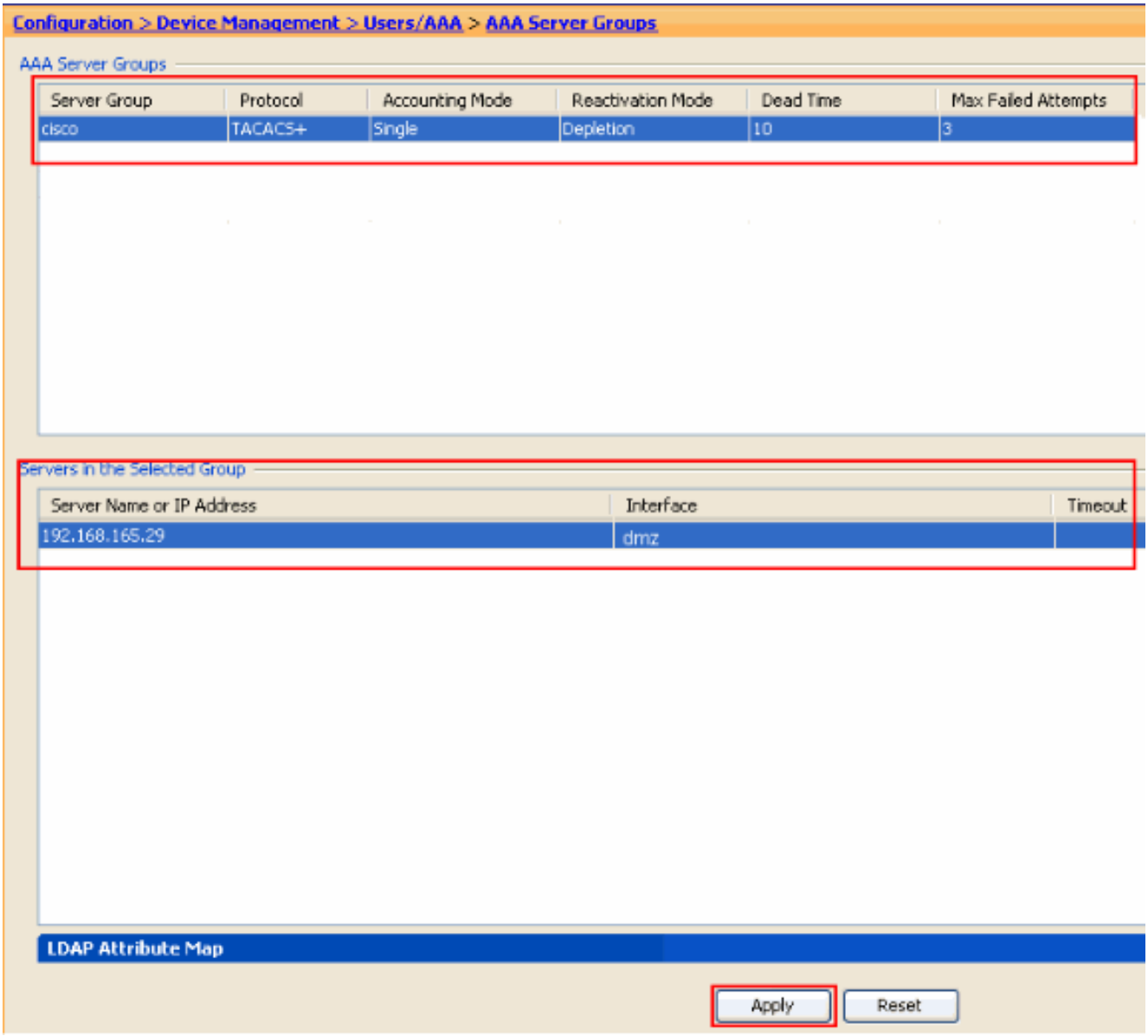


4. Предоставьте подробную информацию **AAA-сервера** в окне **Add AAA Server** как показано. Используемая группа серверов является

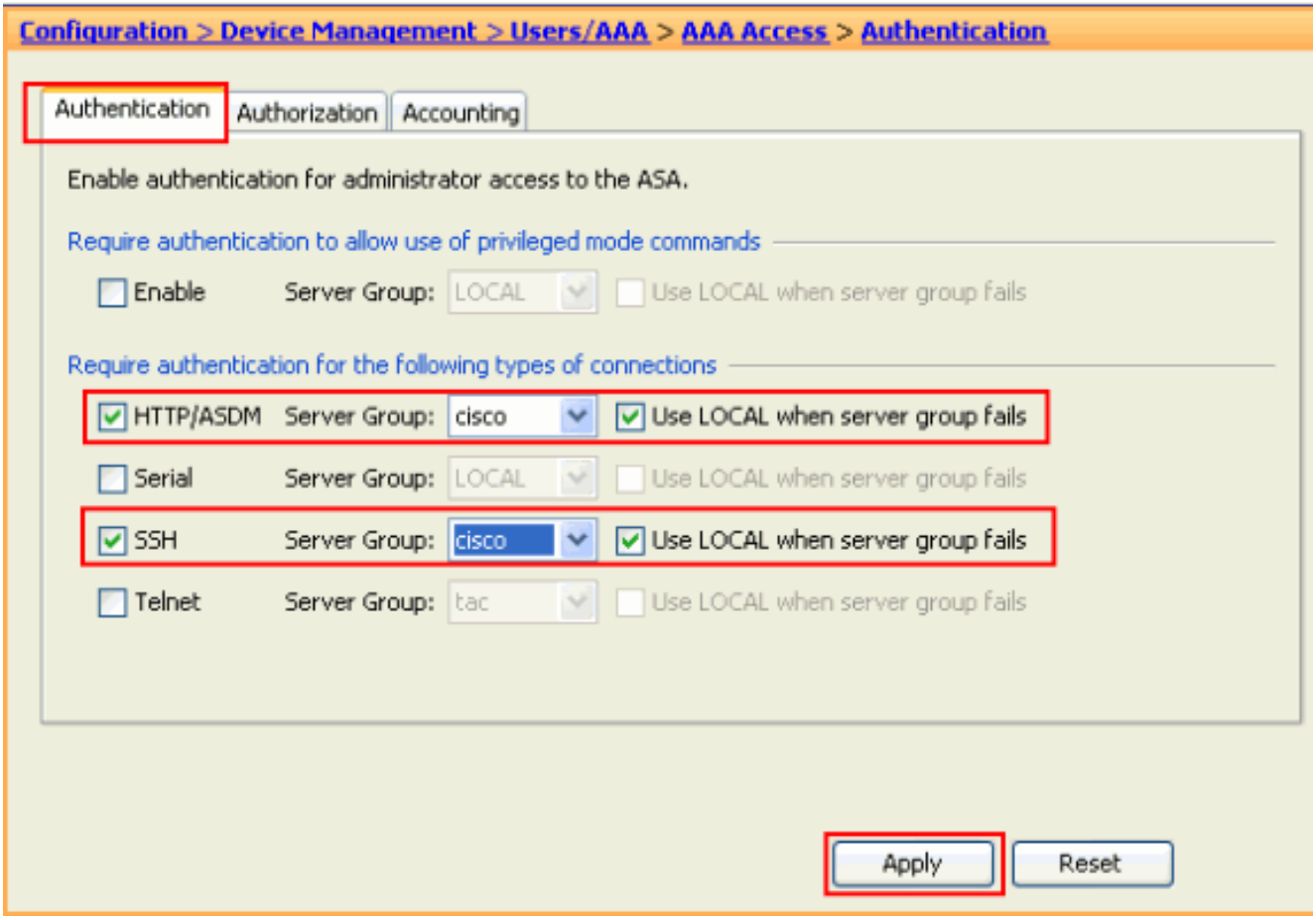


Cisco. **Нажмите OK**, затем нажмите **Apply**.Вы будете видеть **Группу AAA-серверов** и **AAA-сервер**, настроенный на ASA.

5. **Щелкните "Применить".**



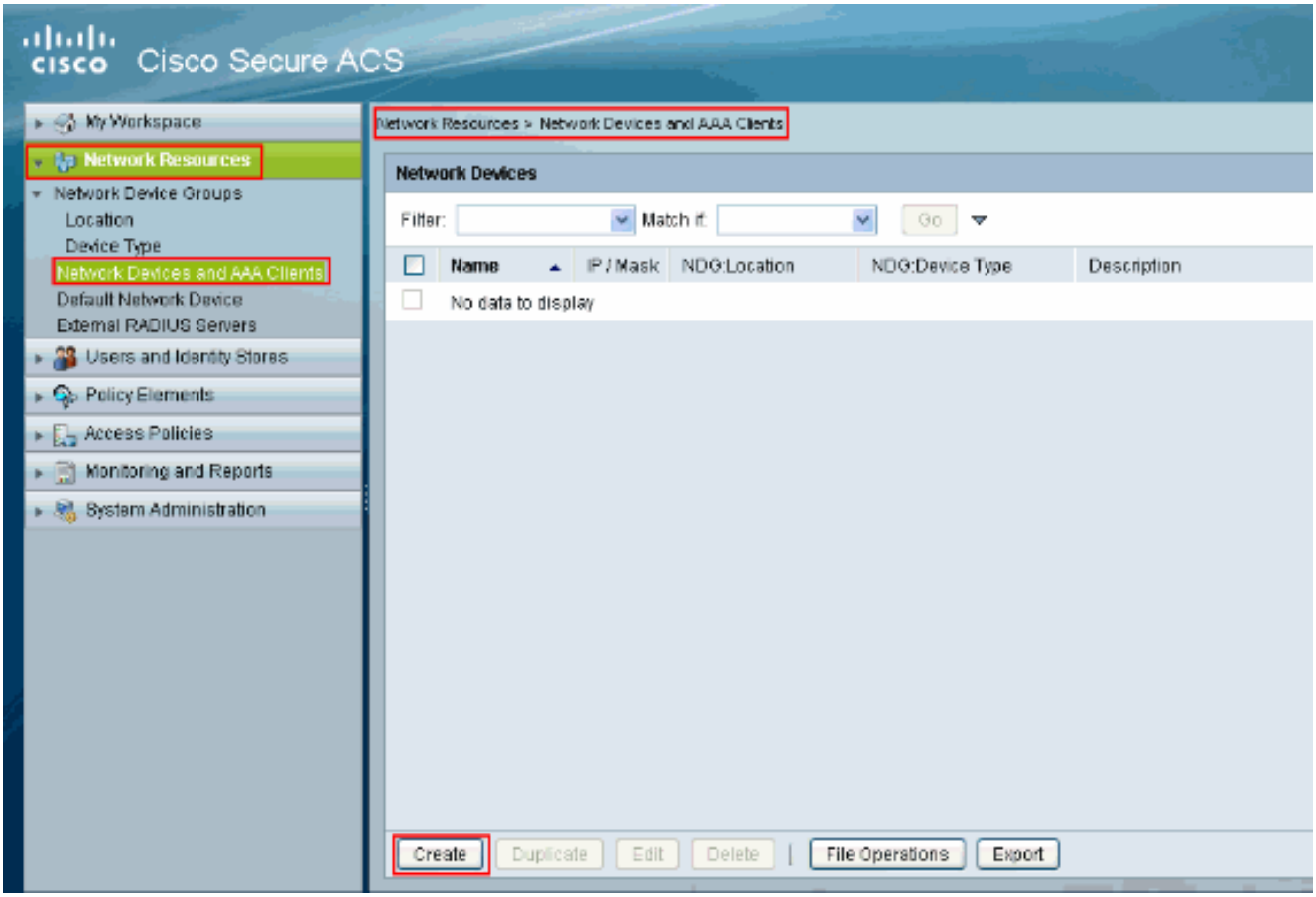
6. Выберите **Configuration>> Users Device Management / AAA> Доступ AAA> Аутентификация** и нажмите флажки, следующие за **HTTP/ASDM** и **SSH**. Затем выберите **Cisco** в качестве группы серверов и нажмите **Apply**.



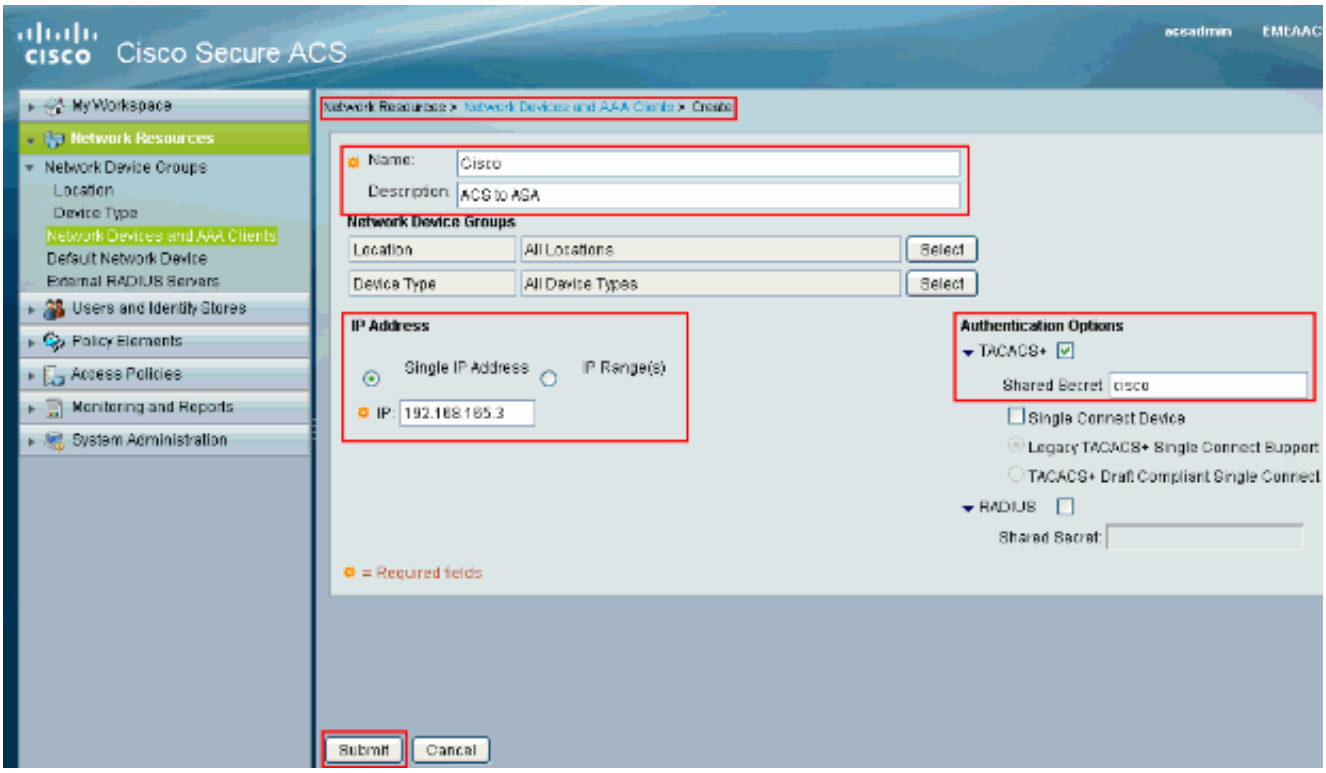
Настройте ACS как СЕРВЕР TACACS

Завершите эту процедуру для настройки ACS как Сервера tacacs:

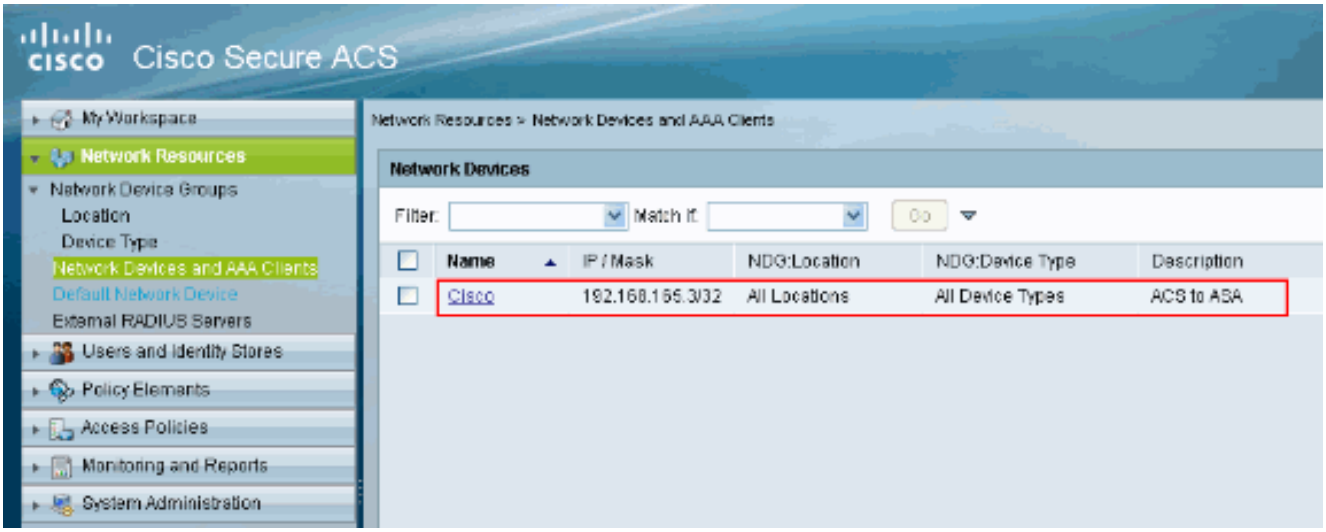
1. Выберите **Network Resources> Network Devices и AAA Clients** и нажмите **Create** для добавления ASA к серверу
   ACS.



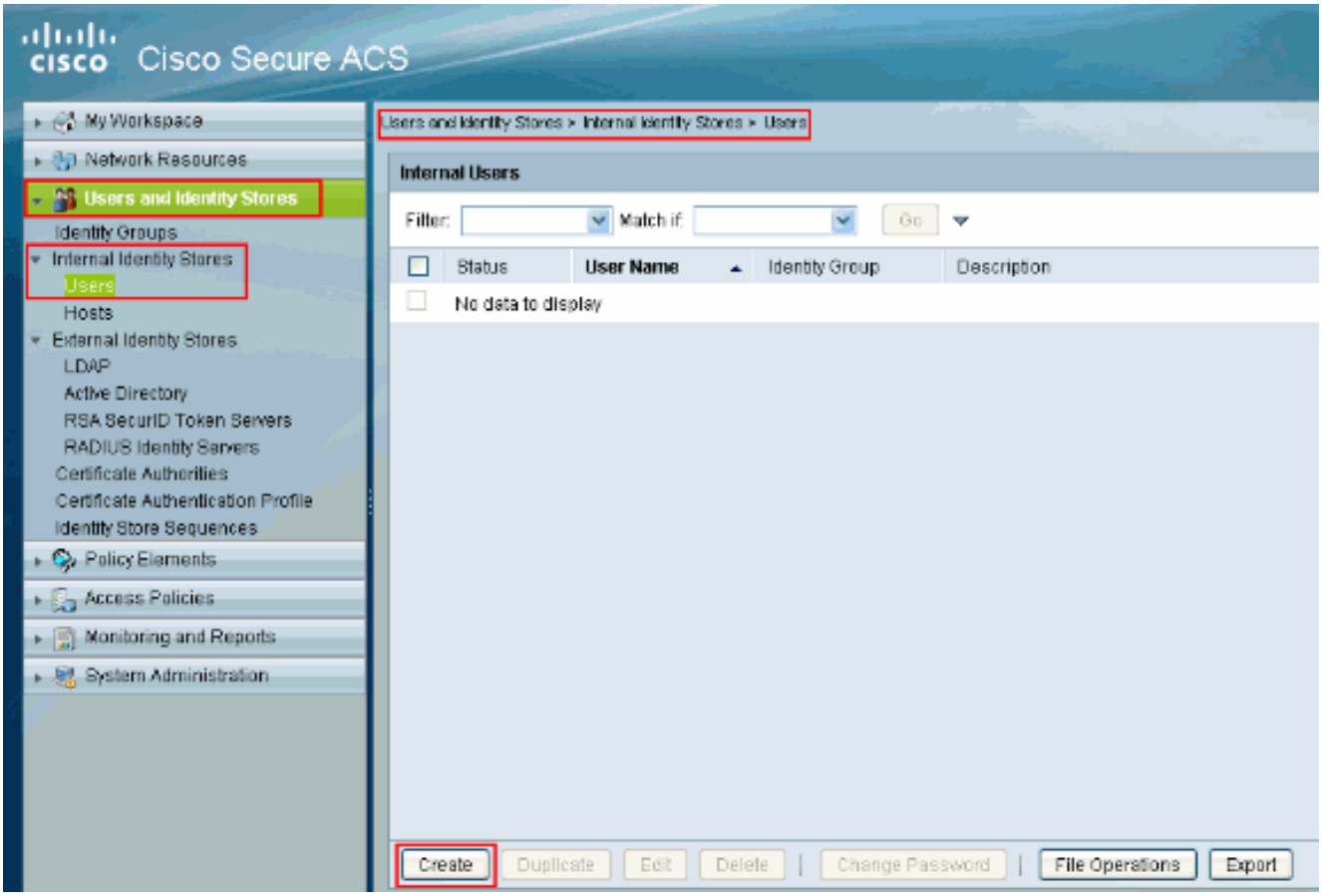
2. Предоставьте необходимую информацию о **клиенте** (ASA является клиентом здесь), и нажмите **Submit**. Этот enablesthe ASA, который будет добавлен к серверу ACS. Подробные данные включают **IP-адрес** ASA и подробных данных **Сервера tacacs**.



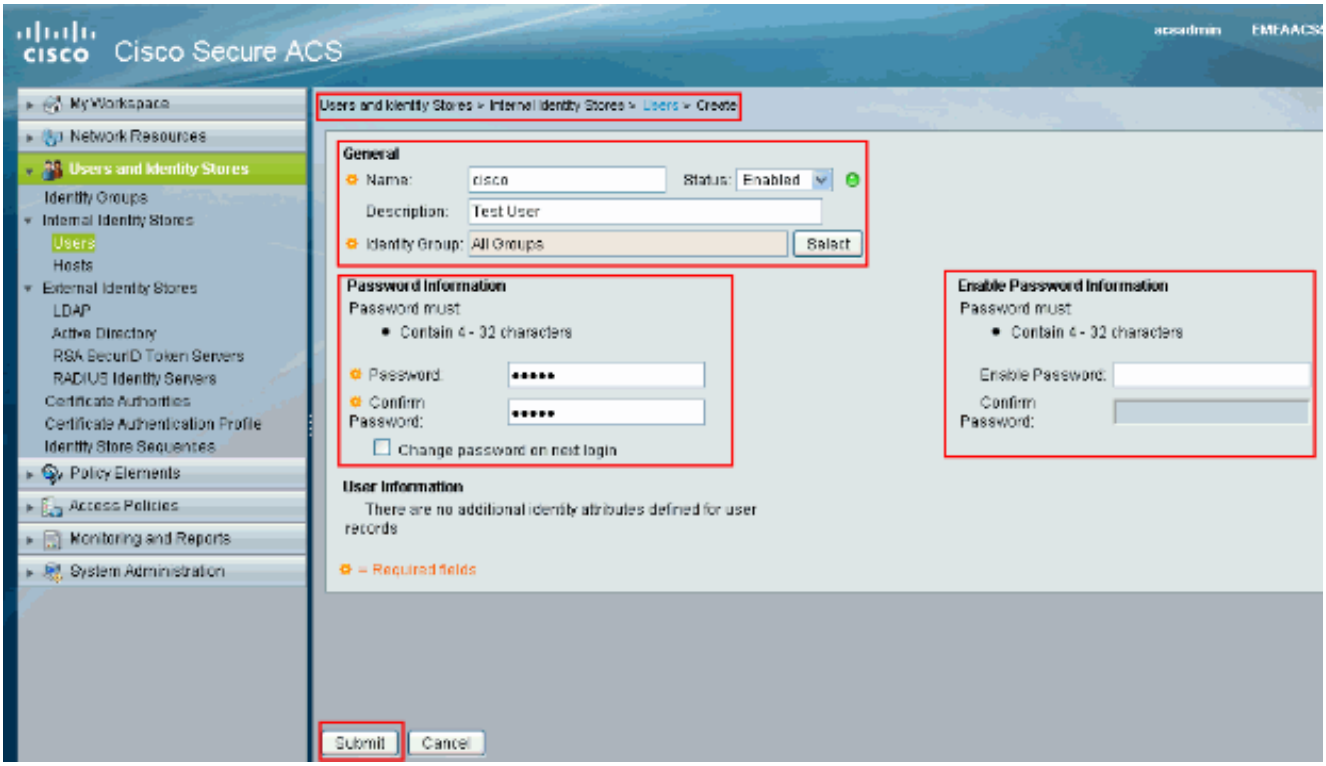
Вы будете видеть, что клиентская **Cisco** добавлена к серверу ACS.



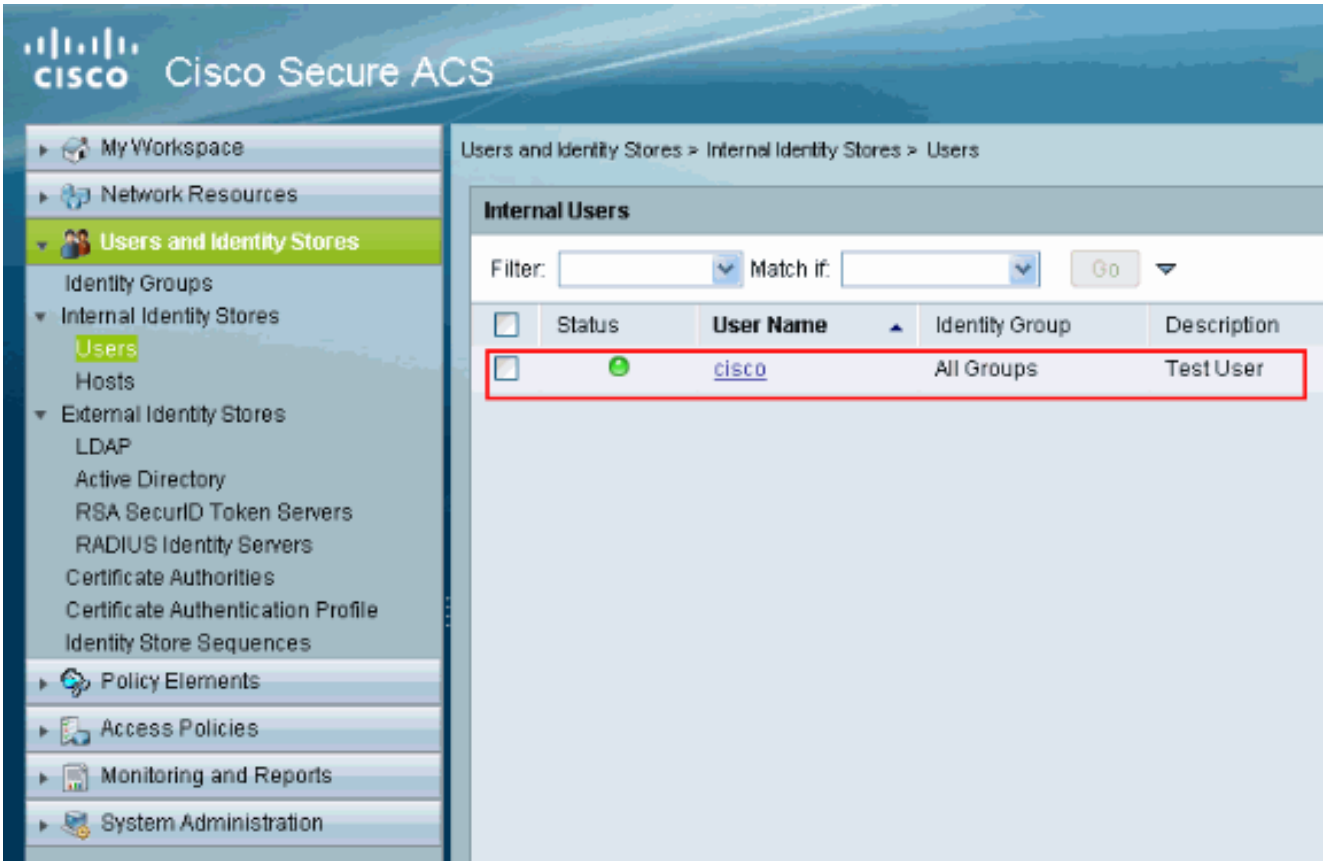
3. Выберите **Users и хранилища Identity> Внутренний Идентификационный> Users Хранилищ** и нажмите **Create** для создания нового пользователя.



4. Предоставьте **Название, Пароль и** информацию **о Enable password. Enable Password** является **дополнительным. По завершении нажмите кнопку Submit (Отправить).**



Вы будете видеть, что пользовательский **Cisco** добавлен к серверу ACS.

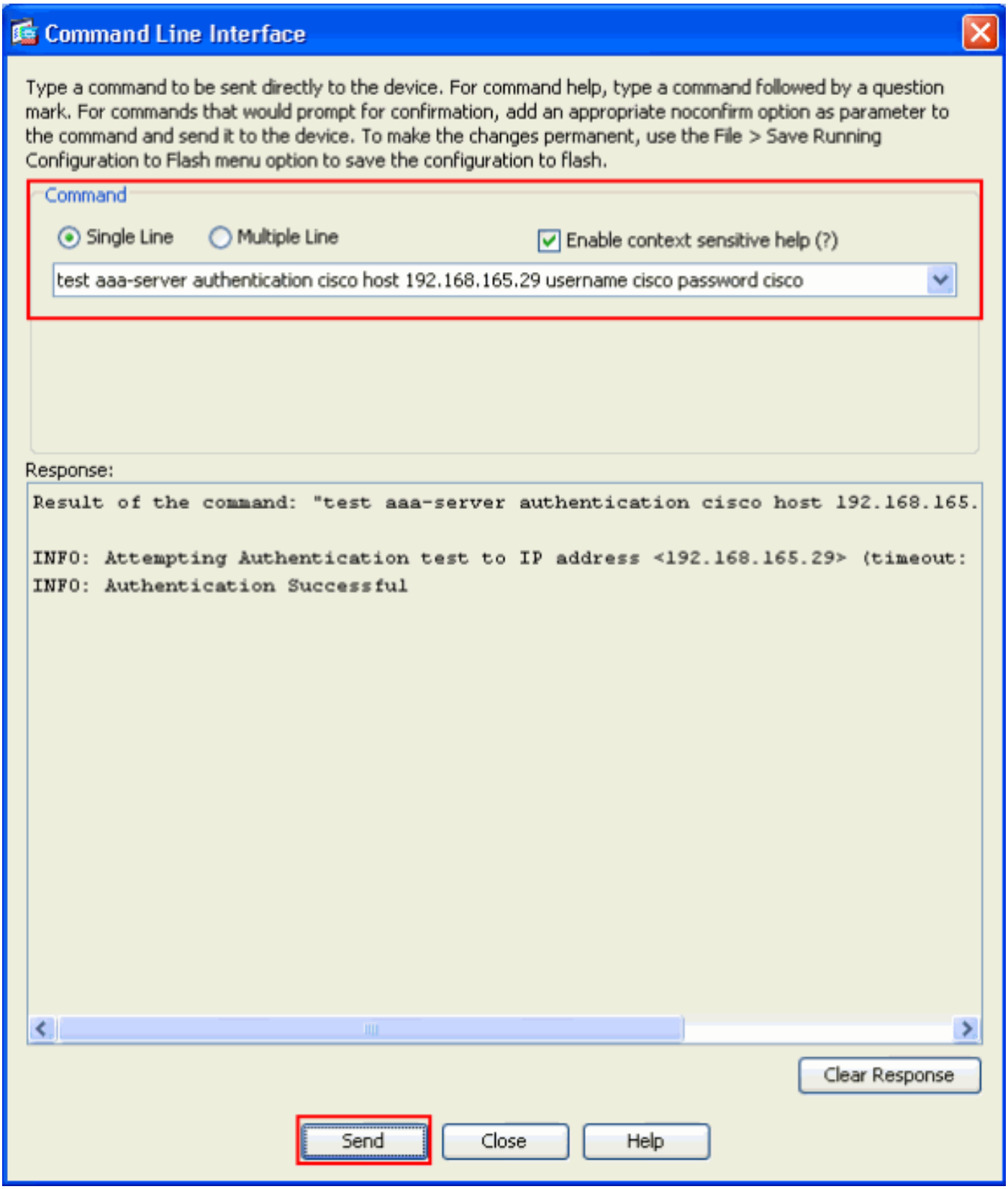


Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Используйте **thetest** команду **пароля cisco имени пользователя cisco хоста 192.168.165.29 Cisco аутентификации aaa-server**, чтобы проверить, работает ли конфигурация должным образом. Этот образ показывает, что аутентификация успешна, и пользователь,

соединяющийся с ASA, аутентифицировался сервером ACS.



Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Устранение неполадок

Ошибка: TACACS маркирующего AAA + сервер x. x. x. x в групповом TACACS aaa-server, как ПОДВЕДЕНО

Это сообщение означает, что Cisco ASA потерял подключение с x. x. x. X-сервер. Удостоверьтесь, что у вас есть допустимое подключение на TCP 49 к серверу x. x. x. x от ASA. Можно также увеличить таймаут на ASA для TACACS + сервер от 5 до необходимого номера секунд в случае, если существует задержка сети. ASA не передал бы запрос аутентификации к Серверу с ошибкой x. x. x. x. Однако это будет использовать следующий сервер в групповом TACACS aaa-server.

Дополнительные сведения

- Страница поддержки устройств адаптивной безопасности Cisco ASA серии 5500
- Справочники по командам устройств адаптивной защиты Cisco ASA серии 5500
- Диспетчер адаптивных устройств защиты Cisco (Cisco Adaptive Security Device Manager)
- Страница технической поддержки протоколов согласования IPSec и IKE
- Cisco Secure Access Control Server for Windows
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация