

# Интеграция ACS Version 5.x с примером конфигурации WAAS

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Настройка](#)

[Настройте ACS](#)

[Конфигурация на WAAS](#)

[Проверка](#)

[Устранение неполадок](#)

## Введение

Этот документ описывает, как настроить интеграцию Сервисов WAAS (WAAS) Cisco с Версией 5 Access Control Server (ACS) Cisco. x. Когда настроено на шаги в этот документ, пользователи в состоянии аутентифицироваться на WAAS с TACACS + учетные данные через ACS.

## Предварительные условия

### Требования

Для этого документа отсутствуют особые требования.

### Используемые компоненты

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

- Версия 5 Cisco Secure ACS. x
- Cisco WAAS

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.

# Настройка

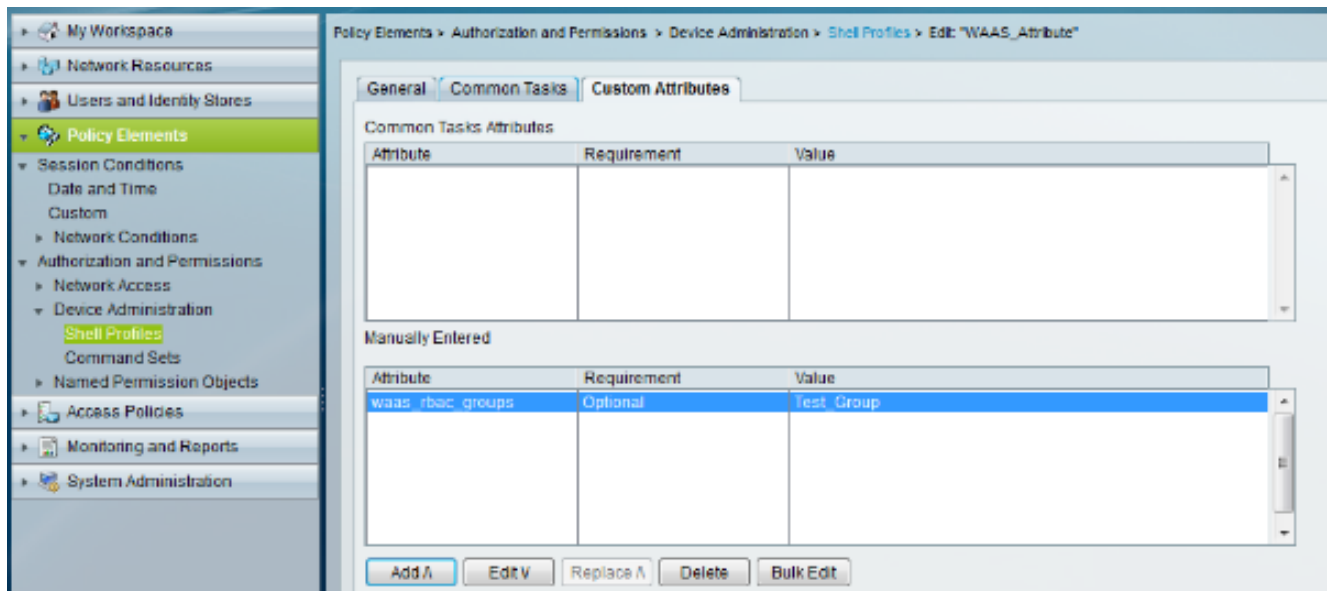
## Настройте ACS

1. Для определения клиента AAA на ACS Version 5.x перейдите к **Сетевым ресурсам**> **Сетевые устройства и Клиенты AAA**. Настройте клиента AAA с описательным именем, одним IP-адресом и общим секретным ключом для TACACS +.

The screenshot shows the 'Create' page for a new AAA client in the Cisco ACS 5.x web interface. The left sidebar contains a navigation tree with 'Network Resources' expanded to 'Network Devices and AAA Clients'. The main content area is titled 'Network Resources > Network Devices and AAA Clients > Create'. The form includes the following fields and options:

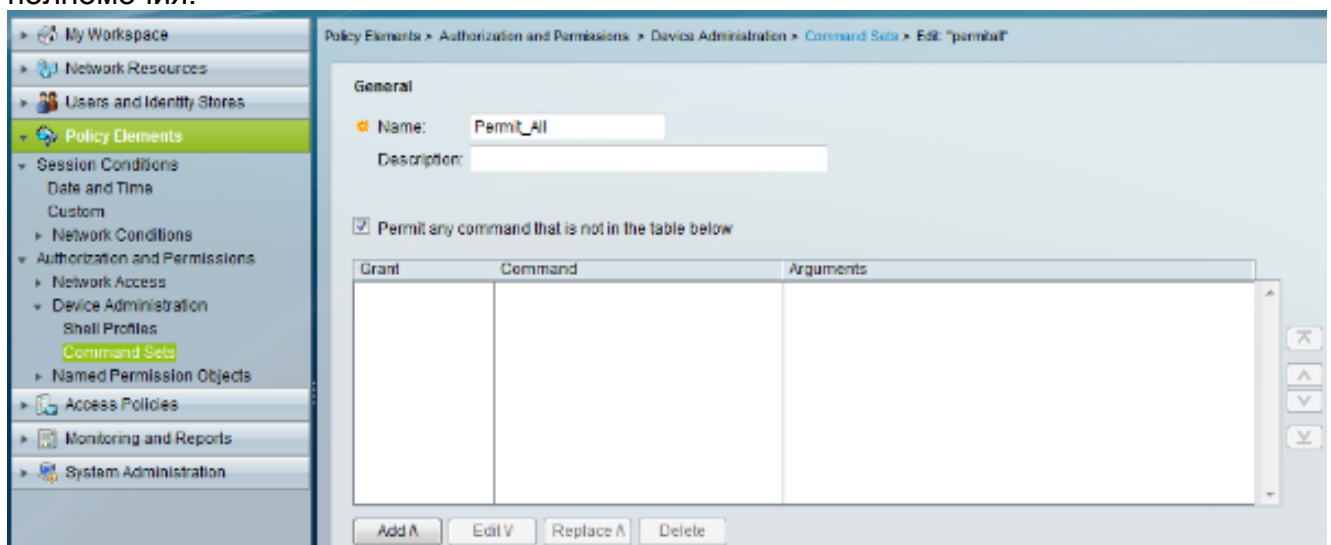
- Name:** WAAS
- Description:** test AAA client
- Network Device Groups:**
  - Location:** All Locations (with a 'Select' button)
  - Device Type:** All Device Types (with a 'Select' button)
- IP Address:**
  - Radio buttons for **Single IP Address** (selected), **IP Subnets**, and **IP Range(s)**.
  - IP:** 1.1.1.1
- Authentication Options:**
  - TACACS+:** Checked. **Shared Secret:** disc0 (with a 'Hide' button).
  - Single Connect Device
  - Legacy TACACS+ Single Connect Support
  - TACACS+ Draft Compliant Single Connect Support
  - RADIUS:** Unchecked.
  - Shared Secret:** (with a 'Show' button)
  - CoA port:** 1700
  - Enable KeyWrap
  - Key Encryption Key:** (empty field)
  - Message Authenticator Code Key:** (empty field)
  - Key Input Format:**  ASCII  HEXADECIMAL

2. Для определения Профиля Shell перейдите к **Элементам Политики**> **Авторизация и Разрешения**> **Администрирование устройств**> **Профили Shell**. В данном примере настроен новый профиль оболочки под названием **WAAS\_Attribute**. Этот настраиваемый атрибут передается WAAS, который позволяет ему выводить, какая группа пользователей является группой администраторов. Настройте эти настраиваемые атрибуты:  
**Атрибут** является **waas\_rbac\_groups**. **Требование** является **Дополнительным** так, чтобы оно не нарушало никакое другое устройство. **Значение** является названием группы, которая должна быть назначенным административным доступом (Test Group).



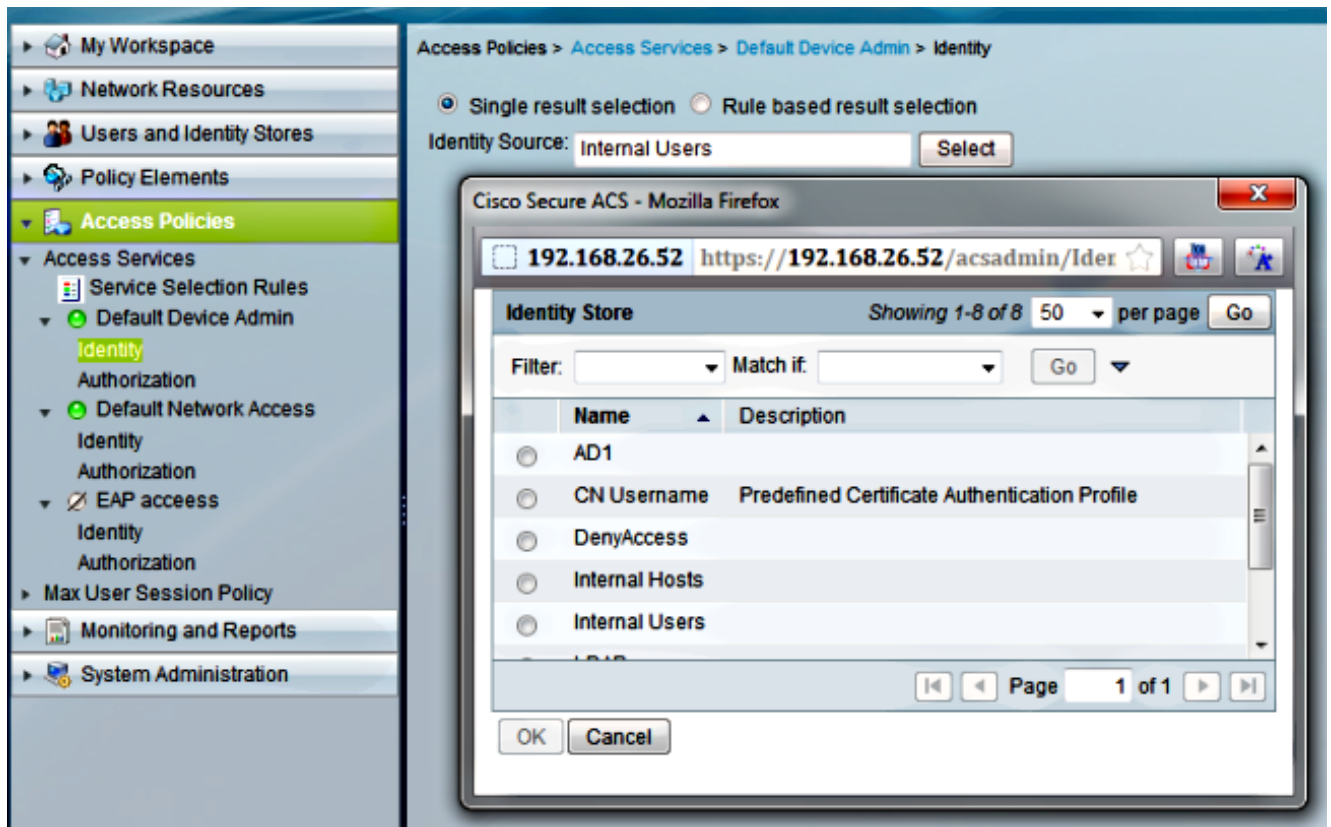
3. Для определения набора команд, чтобы позволить все команды, перейти к **Элементам Политики > Авторизация и Разрешения > Администрирование устройств > Наборы команд**.

Отредактируйте набор команд **Permit\_All**. Если вы проверяете **Разрешение** какая-либо команда, которая не находится в таблице ниже флажка, пользователю предоставляют полные полномочия.

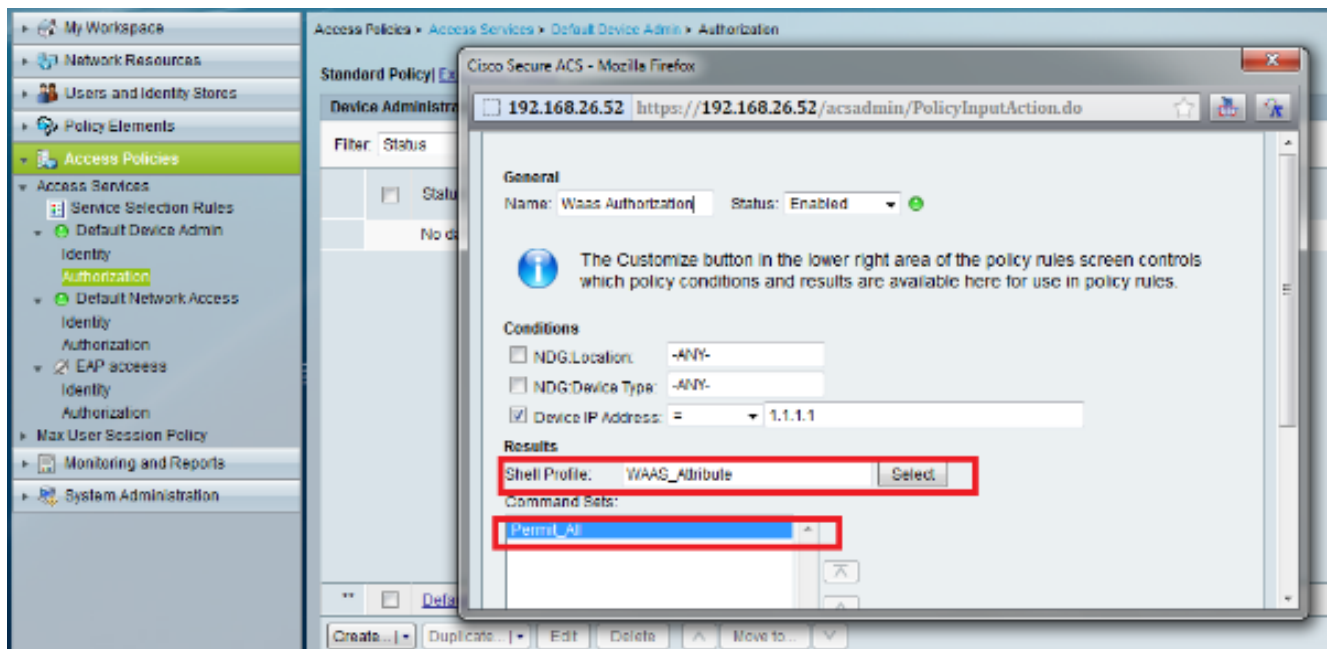


**Примечание:** Так как данный пример использует TACACS, выбранный сервис по умолчанию является **администратором устройства по умолчанию**.

4. Для обращения идентичности к корректному идентификационному источнику перейдите к **Политике доступа > Службы доступа > Администратор устройства по умолчанию > Идентичность**. Если пользователь существует в локальной базе данных ACS, выберите **Internal Users**. Если пользователь существует в Active Directory, выберите настроенное идентификационное хранилище (**AD1** в данном примере).



- Для создания правила авторизации перейдите к **Политике доступа > Службы доступа > Администратор устройства по умолчанию > Авторизация**. Создайте новую политику авторизации под названием **Авторизация WAAS**. Это проверяет для запросов от WAAS. В данном примере IP устройства используется в качестве условия. Однако это может быть изменено на основе требований развертываний. Примените профиль оболочки и наборы команд, настроенные в Шагах 2 и 3 в этот раздел.



## Конфигурация на WAAS

- Для определения TACACS + сервер, перейдите к **Устройствам > <Центральное Имя системы Менеджера>> Настраивает > Security > AAA > TACACS +**. Настройте IP-адрес сервера ACS и предварительный общий ключ.

Devices > pi-wavecm01 > Configure > Security > AAA > TACACS+

TACACS+ Server Settings for Central Manager, [redacted] Print Apply Defaults Remove Settings

**TACACS+ Server Settings**

Use ASCII Password Authentication:

Time to Wait:  (seconds) (1-20)

Number of Retransmits:  (1-3)

Security Word:

Primary Server:  Primary Server Port:

Secondary Server:  Secondary Server Port:

Tertiary Server:  Tertiary Server Port:

\* To use TACACS+ for Login or Configuration Authentication, please go to the Authentication Methods page.

2. Для изменения методов проверки подлинности и авторизация перейдите к **Устройствам > <Центральное Имя системы Менеджера> Настраивает > Security > AAA > Методы аутентификации**. В этом снимке экрана основной способ входа в систему настроен для **локальной переменной** со вторичным устройством, настроенным для **TACACS +**.

Devices > pi-wavecm01 > Configure > Security > AAA > Authentication Methods

Authentication and Authorization Methods for Central Manager, pi-wave... Print Apply Defaults Remove Settings

**Authentication and Authorization Methods**

Failover to next available authentication method:

Authentication Login Methods:  It is highly recommended to set the auther

Primary Login Method:

Secondary Login Method:

Tertiary Login Method:

Quaternary Login Method:

Authorization Methods:

Primary Configuration Method:

Secondary Configuration Method:

Tertiary Configuration Method:

Quaternary Configuration Method:

3. Перейдите к **Дом > Admin > AAA > Группы пользователей** для добавления имени группы, которое совпадает со **Значением** настраиваемого атрибута (см. Шаг 2 в **Настраивать** раздел **ACS**) в **WAAS**.

Home > Admin > AAA > User Groups

**Creating New User Group** Print

---

**User Group Information**

Name:

---

**Comments**

---

Note: \* - Required Field

4. Назначьте эту группу (Test\_Group) права **уровня admin** на вкладке **Home> Admin> AAA> User Groups Role Management**. Роль **admin** на Центральном Менеджере предварительно сконфигурирована.

Home > Admin > AAA > User Groups

External User Group Management **Role Management** Domain Management

Refresh Table Assign all Roles Remove all Roles

**Roles**

Filter: Name  Match if: like

Role	
admin	Admin role

## Проверка

Попытка войти в систему WAAS с TACACS + учетные данные. Если все настроено правильно, вы - предоставленный доступ.

## Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.