

Интеграция NCS с примером конфигурации ACS 5.4

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Настройка](#)

[Добавьте ACS как СЕРВЕР TACACS](#)

[Параметры настройки режима AAA](#)

[Конфигурация версии ACS 5.4](#)

[Проверка](#)

[Устранение неполадок](#)

Введение

Этот документ предоставляет пример конфигурации для TACACS + проверка подлинности и авторизация на Cisco Главный Выпуск 1.1 Системы управления сетью (NCS).

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Определите NCS как клиента в Системе управления доступом (ACS).
- Определите IP-адрес и идентичный разделяемый секретный ключ на ACS и NCS.

Используемые компоненты

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

- Версия ACS 5.4

- NCS главный выпуск 1.1

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

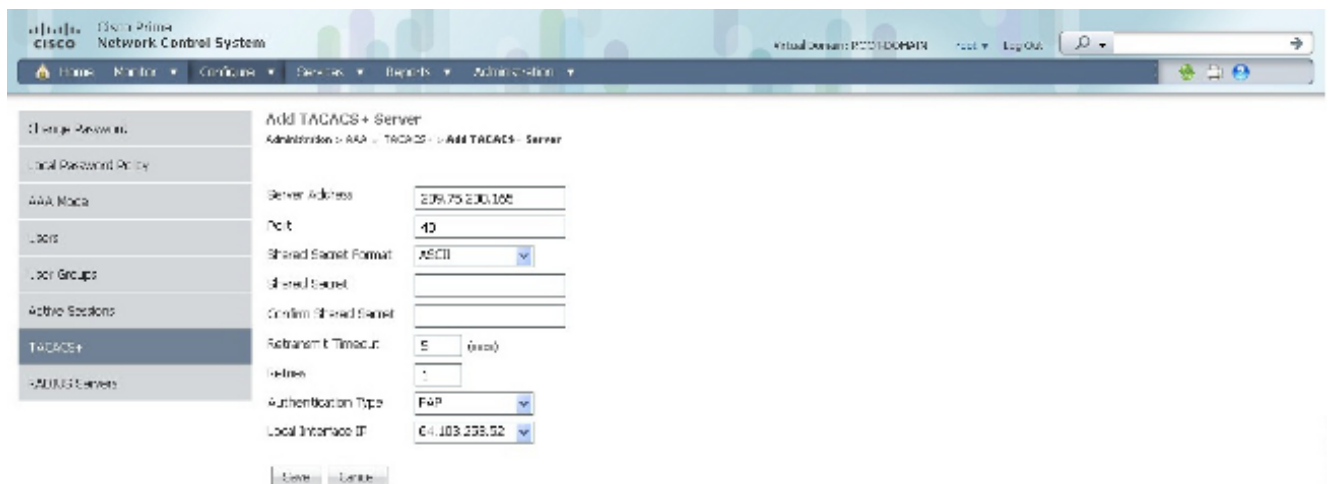
В этом разделе вам предоставляют информацию, используемую для настройки функций, описанных в этом документе.

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

Добавьте ACS как СЕРВЕР TACACS

Выполните эти шаги для добавления ACS как Сервера tacacs:

1. Перейдите к **администрированию > AAA**.
2. Из левого меню боковой панели выберите **TACACS +**, и это отображения информации:



The screenshot shows the Cisco Prime Network Control System interface. The left sidebar contains a navigation menu with options like 'Change Password', 'Local Password Policy', 'AAA Mode', 'Local Groups', 'Active Sessions', 'TACACS+', and 'RADIUS Servers'. The 'TACACS+' option is selected. The main content area is titled 'Add TACACS+ Server' and shows the configuration for a server named 'AAA TACACS+ Server'. The fields are filled with the following values: Server Address: 109.75.230.100; Port: 49; Shared Secret Format: ASCII; Shared Secret: (empty); Confirm Shared Secret: (empty); Retransmit Timeout: 5 (secs); Timeout: (empty); Authentication Type: PAP; Local Interface IP: 10.103.238.32. There are 'Save' and 'Cancel' buttons at the bottom.

Страница TACACS + показывает, что IP-адрес, порт, повторно передает скорость и тип проверки подлинности.

3. Добавьте IP-адрес сервера ACS.
4. Введите TACACS + общий секретный ключ, используемый сервером ACS.
5. Повторно войдите в общий секретный ключ в **Подтвердить** текстовом поле **Общего секретного ключа**.
6. Остаток выхода полей на их настройке по умолчанию.

7. Нажмите кнопку Submit (Отправить).

Параметры настройки режима AAA

Для выбора режима Authentication, Authorization, and Accounting (AAA) выполните эти шаги:

1. Перейдите к **администрированию> AAA**.
2. Выберите **AAA Mode** из левого меню боковой панели и этого отображения информации:



3. Выберите **TACACS +**.
4. Проверьте **Разрешать Нейтрализацию к Локальному** флажку, если вы хотите, чтобы администратор использовал локальную базу данных, когда внешний AAA-сервер (ACS) не работает. Это рекомендуется так, чтобы аутентификация все еще произошла, если отказывает TACACS + сервер. Как только конфигурация проверена и работает, можно внести изменения при желании.

Конфигурация версии ACS 5.4

Для конфигурации Версии ACS 5.4 необходимо выполнить эти шаги для передачи атрибутов от ACS до NCS:

1. Получите атрибуты:

Перейдите к **администрированию> AAA> Группы пользователей**.

Данный пример показывает проверку подлинности администратора. Ищите **Название Admin Group** в списке и нажмите опцию **Task List** справа.

Group Name	Members	Multi-val	Export
Admin	User_admin, isppatl, task20	<input checked="" type="checkbox"/>	Task List
Config Managers	User_cm	<input checked="" type="checkbox"/>	Task List
Lobby Ambassador	User_la	<input checked="" type="checkbox"/>	Task List
Monitor Lite	User_ml	<input checked="" type="checkbox"/>	Task List
Northbound API	User_nb	<input checked="" type="checkbox"/>	Task List
Root	root	<input checked="" type="checkbox"/>	Task List
Super User	User_su	<input checked="" type="checkbox"/>	Task List
System Monitoring	User_sm	<input checked="" type="checkbox"/>	Task List
User Assistant	User_ua	<input checked="" type="checkbox"/>	Task List
User Defined 1		<input checked="" type="checkbox"/>	Task List
User Defined 2		<input checked="" type="checkbox"/>	Task List
User Defined 3		<input checked="" type="checkbox"/>	Task List
User Defined 4		<input checked="" type="checkbox"/>	Task List

Export Task List

Administration > AAA > User Groups > Export Task List

Please cut and paste the appropriate protocol data below into the custom (and/or specific attribute) field in your AAA server TACACS+ Custom Attributes

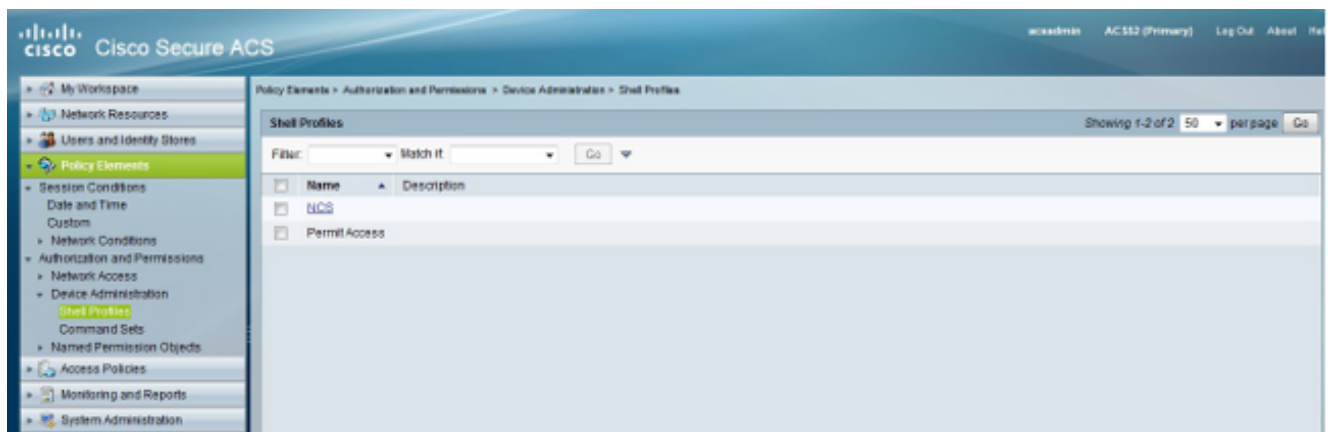
RADIUS Custom Attributes

task0=Admin	NCS:task0=Admin
task0=GLOBAL	NCS:task0=GLOBAL
task1=View Alerts and Events	NCS:task1=View Alerts and Events
task2=Lobby Ambassador Defaults Configuration	NCS:task2=Lobby Ambassador Defaults Configuration
task3=Service Reports	NCS:task3=Service Reports
task4=Monitor Controllers	NCS:task4=Monitor Controllers
task5=Admin Stat Panel Access	NCS:task5=Admin Stat Panel Access
task6=RADIUS Servers	NCS:task6=RADIUS Servers
task7=Monitor Security	NCS:task7=Monitor Security
task8=Monitor Health Access	NCS:task8=Monitor Health Access
task9=Network Summary Reports	NCS:task9=Network Summary Reports
task10=Configure ACS View Servers	NCS:task10=Configure ACS View Servers
task11=Run Reports Link	NCS:task11=Run Reports Link
task12=View GAS Configurations Only	NCS:task12=View GAS Configurations Only
task13=Administration Health Access	NCS:task13=Administration Health Access
task14=Monitor Clients	NCS:task14=Monitor Clients
task15=Configure Switch Location Configuration Templates	NCS:task15=Configure Switch Location Configuration Templates
task16=Monitor Interference	NCS:task16=Monitor Interference
task17=Configure WiFi TD04 Receivers	NCS:task17=Configure WiFi TD04 Receivers
task18=Configure Guest Users	NCS:task18=Configure Guest Users
task19=TAC Case Attachment Tool	NCS:task19=TAC Case Attachment Tool
task20=Configure HighSpeed Access Point Templates	NCS:task20=Configure HighSpeed Access Point Templates
task21=Monitor Checkpoint	NCS:task21=Monitor Checkpoint
task22=Export Panel Data	NCS:task22=Export Panel Data
task23=View Audit Reports	NCS:task23=View Audit Reports
task24=Configure Access Points	NCS:task24=Configure Access Points
task25=Global SSID Groups	NCS:task25=Global SSID Groups
task26=Report Run History	NCS:task26=Report Run History
task27=Compliance Reports	NCS:task27=Compliance Reports

2. Экспортируйте и сохраните атрибуты к рабочему столу.

3. Войдите к GUI Admin ACS и перейдите к **Элементам Политики > Аутентификация и Разрешения > Администрирование устройств > Профили Shell** для создания Профиля Shell.

4. Назовите профиль NCS.

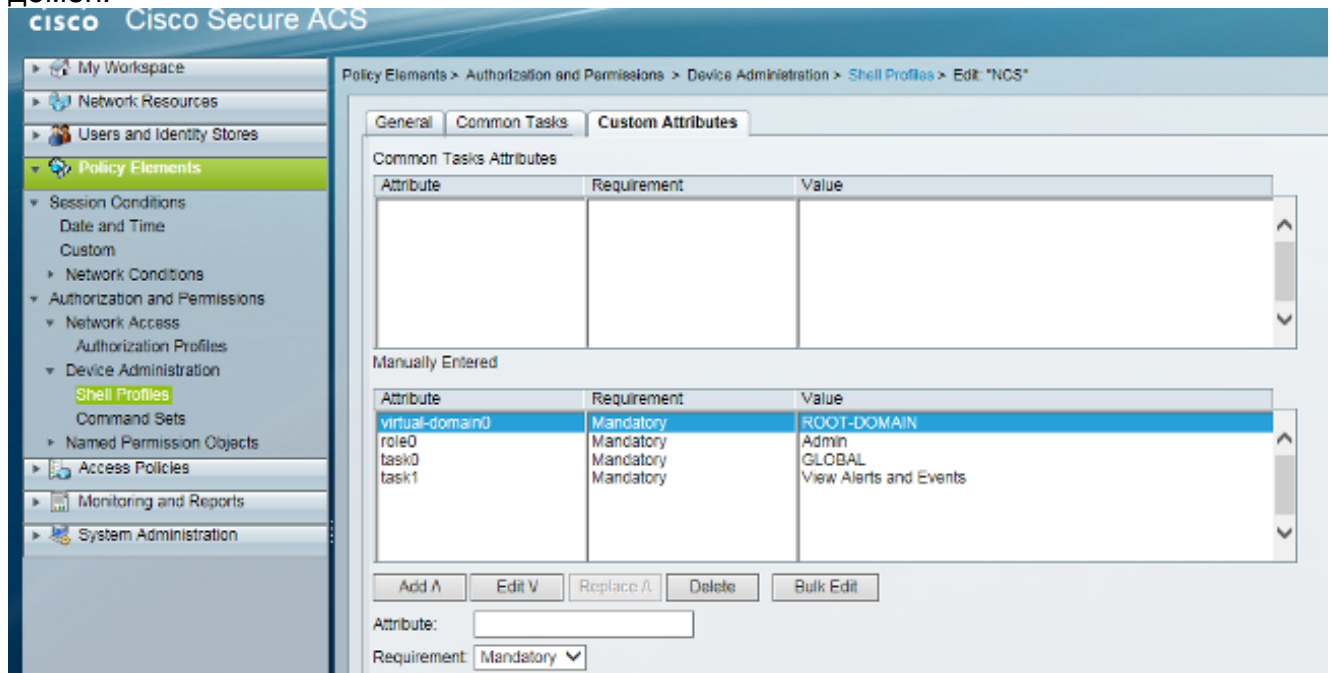


5. От вкладки **Custom Attributes** введите эти значения:

Attribute	Requirement	Value
role0	Mandatory	Admin

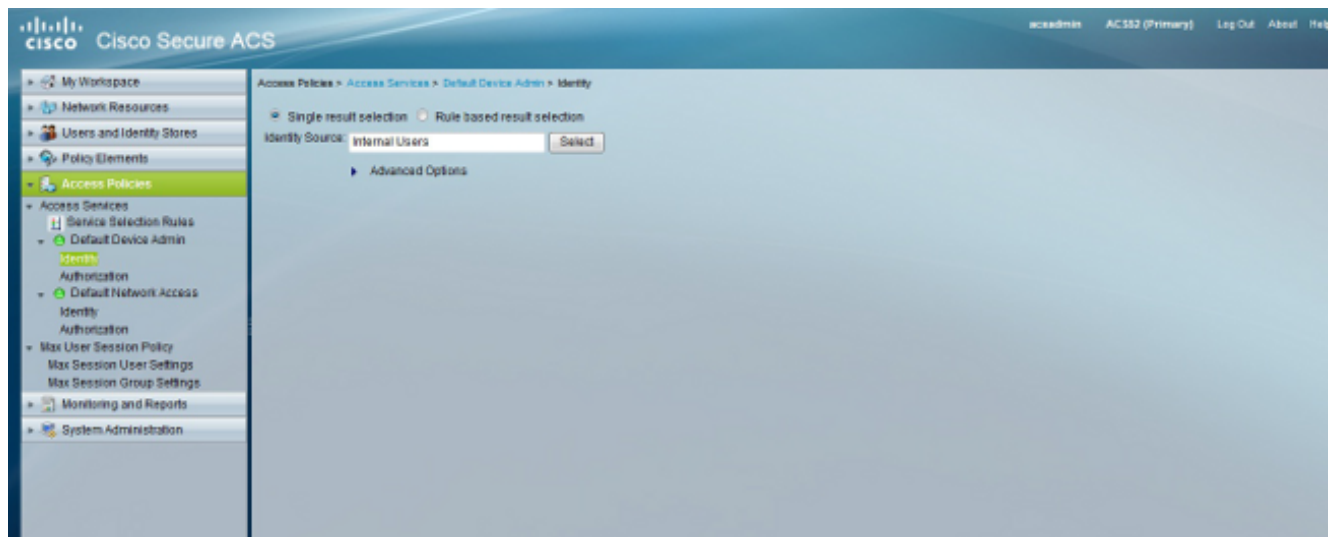
task0	Mandatory	GLOBAL
task1	Mandatory	View Alerts and Events
virtual-domain0	Mandatory	ROOT-DOMAIN

Примечание: Виртуальный домен включен в список в случае, если вы используете последний релиз NCS. Необходимо определить пользовательский виртуальный домен.

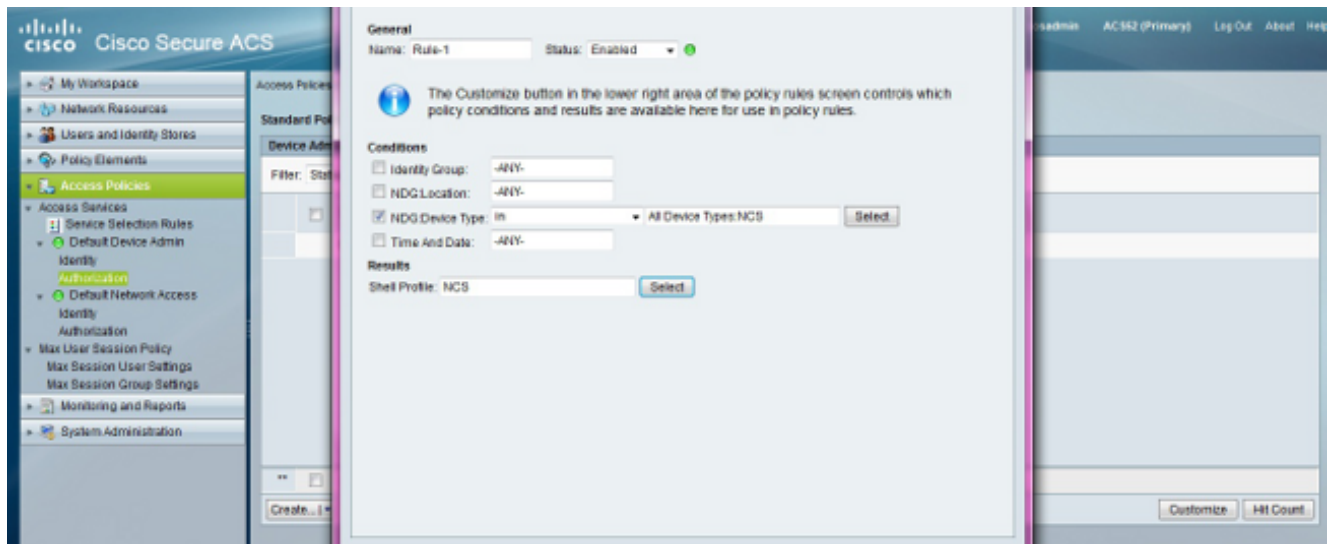


6. Отправьте изменения для создания основанной на атрибуте роли для NCS.

7. Перейдите к Политике доступа > Службы доступа > Администратор устройства по умолчанию > Идентичность и выберите Internal Users для Идентификационного Источника.



8. Создайте новое правило авторизации или отредактируйте правило, которое уже существует в корректной политике доступа. По умолчанию TACACS+ запросы обработаны политикой доступа Администратора устройства по умолчанию.



9. В области **Conditions** выберите соответствующие условия. В области **Results** выберите **NCS** для Профиля Shell.

10. Нажмите кнопку **OK**.

Проверка

Войдите в NCS и подтвердите, что у вас есть роль **Admin**.

Устранение неполадок

Если вы не можете войти в NCS, войдите в GUI ACS и перейдите к **Отслеживанию и сообщению> Каталог> Протоколы AAA (проверка подлинности, авторизация и учет)> TACACS + Аутентификация**. Выберите ошибку проверки подлинности и выберите **Details** для наблюдения, почему была отклонена отказавшая аутентификация или.