# Интеграция версии ACS 5.4 с Motorola WiNGS 5. X (AP) пример конфигурации

## Содержание



## Введение

Этот документ предоставляет примеру конфигурации сервер Cisco Secure Access Control Server (ACS) Версия 5.4 для поддержки TACACS + Аутентификация, авторизация и учет (AAA) на Motorola Wireless Controllers и точках доступа. В этом документе Motorola определяемые поставщиком атрибуты и значения назначены на группы на ACS для определения роли и разрешений доступа каждого пользователя. Атрибуты и значения назначены на группу с определяемыми пользователем сервисами, и протоколы включили на каждой группе.

## Предварительные условия

### Требования

ACS Version 5.x должен быть связан с Motorola WiNGS 5. x.

### Используемые компоненты

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

- Версия ACS 5.4
- WiNGS 5.2

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

### Конфигурация AcS

#### Типы устройства

Вот пример того, как определить Устройства WiNG 5 как типы устройства на Версии 5 Cisco Secure ACS. x. Типы устройства позволяют устройствам быть сгруппированными в Версии 5.x Cisco Secure ACS, которая используется, когда вы определяете политику авторизации устройства.

На GUI ACS перейдите к **Сетевым ресурсам> Группы сетевых устройств> Тип устройства** и нажмите **Create**.

Введите **Имя** и **Описание**, и выберите **Parent**. **Нажмите кнопку Submit (Отправить).**

Это создает **Группу сетевых устройств** для устройств Motorola Solutions.

#### Сетевые устройства и клиенты AAA

Вот пример того, как добавить Устройство WiNG 5 как Клиент AAA на Версии 5 Cisco Secure ACS. x.

На Cisco Secure ACS перейдите к **Сетевым ресурсам> Сетевые устройства и Клиенты AAA**, и нажмите **Create**:

Введите **Имя** для Контроллера (контроллеров) беспроводной локальной сети и выберите **Location**. Назначьте **Тип устройства**, созданный в предыдущем разделе, и проверьте флажок **TACACS +**. Введите **Общий секретный ключ** и нажмите кнопку с зависимой фиксацией рядом с соответствующей **опцией IP Address**. В данном примере выбран **диапазон (диапазоны) IP Маской**, и подсеть IPv4, что Контроллеры беспроводной локальной

сети связаны с **(192.168.20.0/24)**, определена. Нажмите **Submit**, как только вы вводите всю информацию.

Это определяет Контроллер (контроллеры) беспроводной локальной сети как **Сетевые устройства и Клиентов AAA**:

### Identity Groups

В данном примере определены две группы, под названием MotorolaRO и MotorolaRW. Пользователей, назначенных на группу MotorolaRO, назначают на роль Монитора и данные разрешения Веба - доступа, в то время как пользователи назначили на группу MotorolaRW, назначены на роль Суперпользователя и предоставлены Все Разрешения доступа.

Перейдите **Пользователям и Идентификационным Хранилищам>, Identity Groups> Создает**:

Введите **Имя** и **Описание** для группы Доступа только для чтения, и нажмите **Submit.**

Создайте вторую группу. Введите **Имя** и **Описание** для группы Доступа с правом записи Чтения, и нажмите **Submit**.

Вы теперь создали две **Identity Groups**.

### Профили Shell

Вот пример того, как определить профили оболочки на Версии 5 Cisco Secure ACS. x. В данном примере два профиля оболочки, под названием RO MOTO и RW MOTO, определены с атрибутами, которые определяют роль и разрешения доступа, что назначают каждому пользовательскому интерфейсу управления. Название каждого профиля оболочки должно совпасть с названием TACACS + сервис проверки подлинности, определенный в TACACS + политика AAA.

Перейдите к **Элементам Политики> Авторизация и Разрешения> Администрирование устройств> Профили Shell**. **Нажмите кнопку Create.**

На **Вкладке Общие** определите требуемый TACACS + сервисы и протоколы для добавления. Можно использовать текущие сервисы и протоколы или создать собственное. Данный пример определяет сервисы и протоколы под именем RO MOTO для обеспечения Доступа только для чтения к Устройствам WiNG 5:

На вкладке **Common Tasks**, устанавливает **Максимальная Привилегия** в **Статический**, и выбирать значение **1**.

На вкладке **Custom Attributes**, в полях **Attribute и Attribute Value**, определяют атрибуты, которые будут назначены на пользователя. В данном примере пользователей Только для чтения назначают на роль Монитора и данные разрешения Веба - доступа. **Нажмите кнопку Submit (Отправить).**

Создайте новый **Профиль Shell**. На **Вкладке Общие** определите требуемый TACACS + сервисы и протоколы для добавления. Можно использовать текущие сервисы и протоколы или создать собственное. Данный пример определяет сервисы и протоколы, названные RW

MOTO, которые предоставляют Доступ с правом записи Чтения для Устройств WiNG 5:

На вкладке **Common Tasks**, устанавливает **Максимальная Привилегия** в **Статический**, и выбирать значение **1**.

На вкладке **Custom Attributes**, в полях **Attribute и Attribute Value**, определяют атрибуты, которые будут назначены на пользователя. В данном примере пользователей Записи Чтения назначают на роль Суперпользователя и предоставляют Все Разрешения доступа. **Нажмите кнопку Submit (Отправить).**

Вы теперь создали **Профили Shell** под названием RO MOTO и RW MOTO.

### Профили авторизации устройства

Вот пример того, как определить политику авторизации устройства на Версии 5 Cisco Secure ACS. x. Политика авторизации устройства определяет профиль оболочки, каждому пользовательскому интерфейсу управления назначают на основе типа устройства, который запрашивает аутентификацию, местоположение и идентификационный состав группы. В данном примере определена две политики авторизации устройства, под названием MotorolaRO и MotorolaRW.

На Cisco Secure ACS перейдите к **Политике доступа> Администратор устройства по умолчанию>, Авторизация> Настраивает**:

Добавьте Настроить Условия под названием **Identity Group**, **NDG:Location**, **NDG: Тип устройства** и **Протокол**. Под Настраивает Результаты, добавляет **Профиль Shell** и нажимает **OK**:

**Нажмите кнопку Create.** В **Поле имени** введите **MotorolaRO** и выберите **Identity Group**, **NDG:Location** и **NDGevice Type**. Установите Протокол в **Tacacs** и выберите Shell Profile под названием **RO MOTO**. **Нажмите кнопку OK:**

**Нажмите кнопку Create.** В **Поле имени** введите **MotorolaRW** и выберите **Identity Group**, **NDG:Location** и **NDGevice Type**. Установите Протокол в **Tacacs** и выберите Shell Profile под названием **RW MOTO**. **Нажмите кнопку OK:**

Вы теперь создали **Политику авторизации Устройства** под названием MotorolaRO и MotorolaRW:

## Motorola Solutions WiNG 5.2 Configuration

### Политика TACACS AAA

Политика TACACS AAA определяет TACACS + конфигурация клиента на Устройстве WiNG 5. Каждая политика TACACS AAA может содержать до двух TACACS + записи AAA-сервера в дополнение к названиям TACACS + сервис проверки подлинности и протоколы, определенные на Cisco Secure ACS. TACACS + политика AAA также определяет информацию, которая передана к учетному серверу.

Этот пример политики TACACS AAA определяет Cisco Secure ACS для TACACS + AAA, определяет TACACS + сервисы и протоколы под названием RO MOTO и RW MOTO, и включает учет сеанса и команда CLI.

## Пример политики TACACS AAA

```
aaa-tacacs-policy CISCO-ACS-SERVER

authentication server 1 host 192.168.10.21 secret 0 hellomoto

authorization server 1 host 192.168.10.21 secret 0 hellomoto

accounting server 1 host 192.168.10.21 secret 0 hellomoto

authentication service MOTO protocol RO

authentication service MOTO protocol RW

accounting commands

accounting session

!
```

## Политика менеджмента

Однажды TACACS AAA + политика определена, это должно быть назначенный на одну или более политики менеджмента, прежде чем будет использоваться TACACS +. Политика менеджмента определяет интерфейсы управления, которые включены на каждом Устройстве WiNG 5, локальных административных пользователях, ролях и разрешениях доступа, и внешнем RADIUS или TACACS + серверы, используемые для аутентификации административных пользователей.

По умолчанию каждое Устройство WiNG 5 назначено на Политику управления, названную по умолчанию, который назначен с использованием профилей. TACACS + может быть включен на Политике управления по умолчанию или любой определяемой пользователем Политике управления.

Большинство типичных развертываний включает отдельную политику менеджмента для Контроллеров беспроводной локальной сети и точек доступа. Отдельная политика менеджмента рекомендуется, потому что отличаются требования к управлению и интерфейсы для каждого устройства. В этом случае TACACS + должен быть включен на каждой Политике управления для включения TACACS + и на Контроллерах беспроводной локальной сети и на точках доступа.

Примеры Политики управления в следующем разделе включают TACACS + AAA на определяемой пользователем политике менеджмента, которая назначена на Контроллеры беспроводной локальной сети и точки доступа. TACACS + нейтрализация к локальной проверке подлинности также включена, если Устройство WiNG 5 не может достигнуть никакого определенного TACACS + серверы для аутентификации.

## Примеры политики управления

```
!

management-policy CONTROLLER-MANAGEMENT

no http server

https server

ssh

user admin password 0 hellomoto role superuser access all

snmp-server user snmptrap v3 encrypted des auth md5 0 hellomoto

snmp-server user snmpoperator v3 encrypted des auth md5 0 hellomoto

snmp-server user snmpmanager v3 encrypted des auth md5 0 hellomoto

aaa-login tacacs fallback

aaa-login tacacs authorization

aaa-login tacacs accounting

aaa-login tacacs policy CISCO-ACS-SERVER

!

!

management-policy AP-MANAGEMENT

ssh

user admin password 0 hellomoto role superuser access all

aaa-login tacacs fallback

aaa-login tacacs authorization

aaa-login tacacs accounting

aaa-login tacacs policy CISCO-ACS-SERVER

!
```

# Проверка

Этот раздел предоставляет обязательные действия, требуемые для проверки TACACS + AAA. В данном примере две учетных записи пользователя определены на каждом Cisco Secure ACS и назначены на соответствующие группы. Состав группы пользователя определяет роль и разрешения доступа, назначенные на пользовательский интерфейс управления.

```
Username           Role          Access Permissions
--------------------------------------------------
monitor Monitor Web
super user Superuser all
```

## Присвоение роли

Этот раздел предоставляет шаги проверки, требуемые для проверки присвоений роли и аутентификации.

На веб-UI войдите к Контроллеру беспроводной локальной сети с именем пользователя и паролем **монитора**:

Пользователя аутентифицируют, авторизуют и назначают на роль Монитора, которая предоставляет доступ только для чтения на Контроллере беспроводной локальной сети. Выберите **Configuration> Devices** и попытайтесь отредактировать устройство.

> **Примечание:** Никакие не редактируют функциональность, доступно, потому что пользователю разрешают доступ только для чтения.

Доступ на устройстве: (Только **кнопка View** доступна; **кнопка Delete** отображается серым.)

На веб-UI войдите к Контроллеру беспроводной локальной сети с именем пользователя и паролем **суперпользователя**:

Пользователя аутентифицируют, авторизуют и назначают на роль Суперпользователя, которая предоставляет полный доступ на Контроллере беспроводной локальной сети. Выберите **Configuration> Devices** и попытайтесь отредактировать устройство.

> **Примечание: Кнопка Edit** теперь доступна, потому что пользователю разрешают полный доступ на устройстве.

# Устранение неполадок

На Версии 5. X Cisco Secure ACS перейдите к **Отслеживанию и сообщению>, Мониторинг Запуска и Средство просмотра Отчёта> Выбирают Reports> Catalog> AAA Protocol> TACACS Authentication> Run**.

Это представляет результаты для всех, передал и ошибки проверки подлинности для пользователей и включает причину сбоя. Нажмите кнопку (Details) **лупы** для получения дальнейшей информации.