Содержание

Введение

Этот документ объяснит, как создать Tacacs ACS Cisco + профили проверки подлинности и авторизация с другими уровнями привилегий и Интегрировать его с 5760 для доступа к WebUI. Эта функция поддерживается от 3.6.3 и далее (Но не на 3.7.x во время этой записи).

Предварительные условия

Требования

Предполагается, что читатель знаком с ACS Cisco и Сходившейся конфигурацией Контроллера доступа. Этот документ только фокусируется на взаимодействии между теми 2 компонентами в пределах tacacs + авторизация.

Используемые компоненты

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

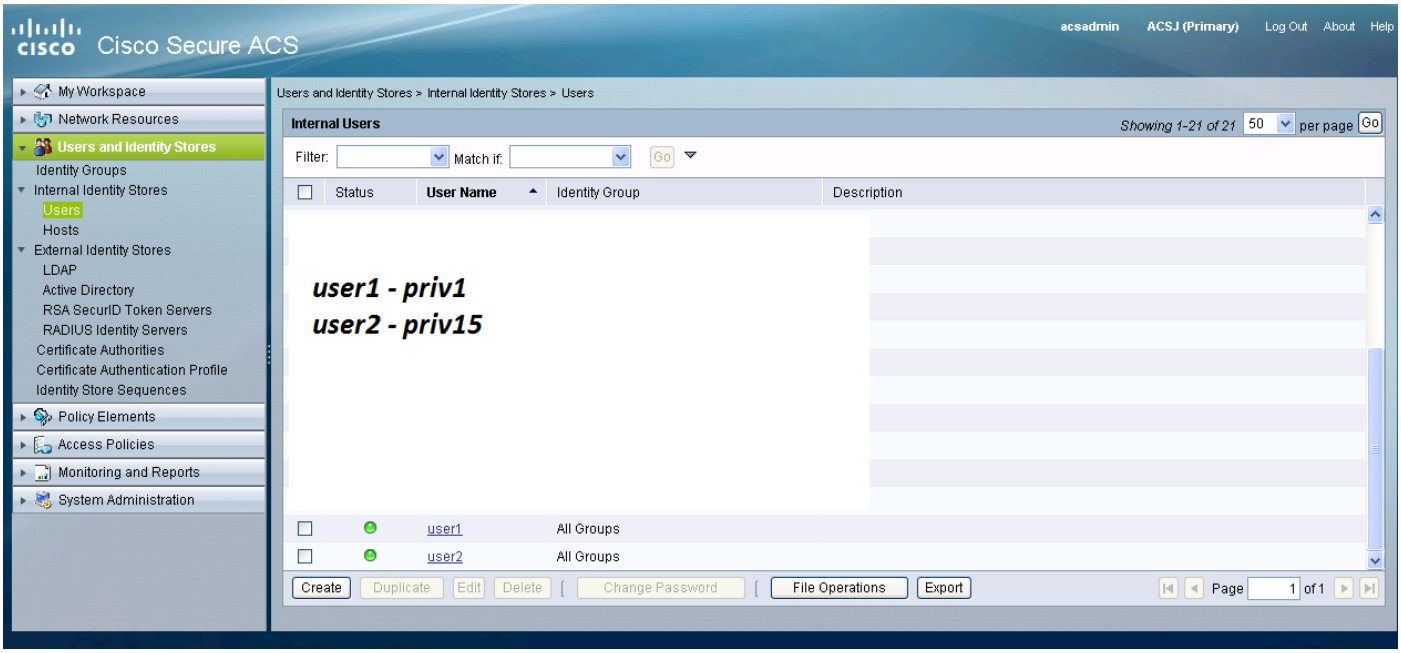
- Cisco Сходилась Доступ 5760, выпуск 3.6.3
- Сервер управления доступом (ACS) Cisco 5.2

!--- конфигурацию

Создайте несколько тестовых пользователей в ACS

Щелкните по "Users and Identity Stores", затем выберите "Users".

Нажмите "Create" и настройте несколько тестовых пользователей такой, как проиллюстрировано ниже.



Устанавливание элементов Политики и профилей оболочки

Необходимо создать 2 профиля для 2 различных типов.Privilege 15 доступа в средствах мира tacacs Cisco предоставить полный доступ устройству без любого ограничения. Привилегия 1, с другой стороны, позволит, что вы, чтобы войти и выполнить только ограниченное количество команд.Below являетесь кратким описанием уровней доступа, предоставленного Cisco.

уровень привилегий 1 = непривилегированный (приглашение является маршрутизатором>), уровень по умолчанию для регистрации

privilege level 15 = privileged (prompt is router#), уровень после входа в режим enable

уровень привилегий 0 = редко используемый, но включает 5 команд: **отключите**, **включите**, **выйдите**, **помогите**, и **выход из системы**

На 5760, уровни 2-14 считают тем же как уровень 1. Им дают ту же привилегию как 1. **Не настраивайте уровни привилегий tacacs для определенных команд на 5760**. Доступ UI на вкладки не поддерживается в 5760. Вы можете или иметь полный доступ (priv15) или только обратиться к вкладке (priv1) Monitor. Кроме того, пользователям с уровнем привилегий 0 не разрешают войти.

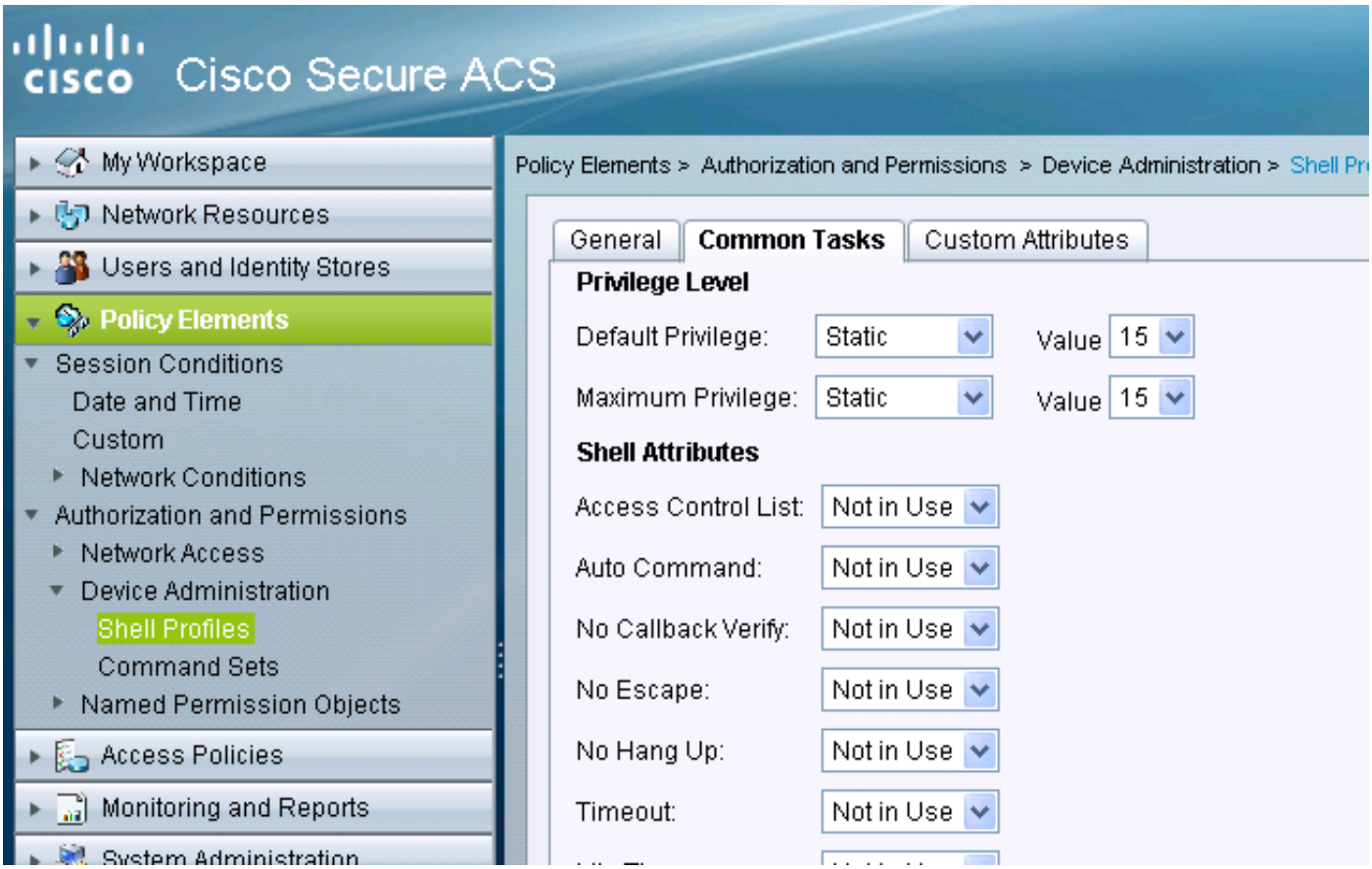
Создание привилегии 15 профилей доступа оболочки уровня

Использование ниже снимка экрана создает тот профиль:

Щелкните по "Policy Elements". Щелкните по "Shell Profiles".

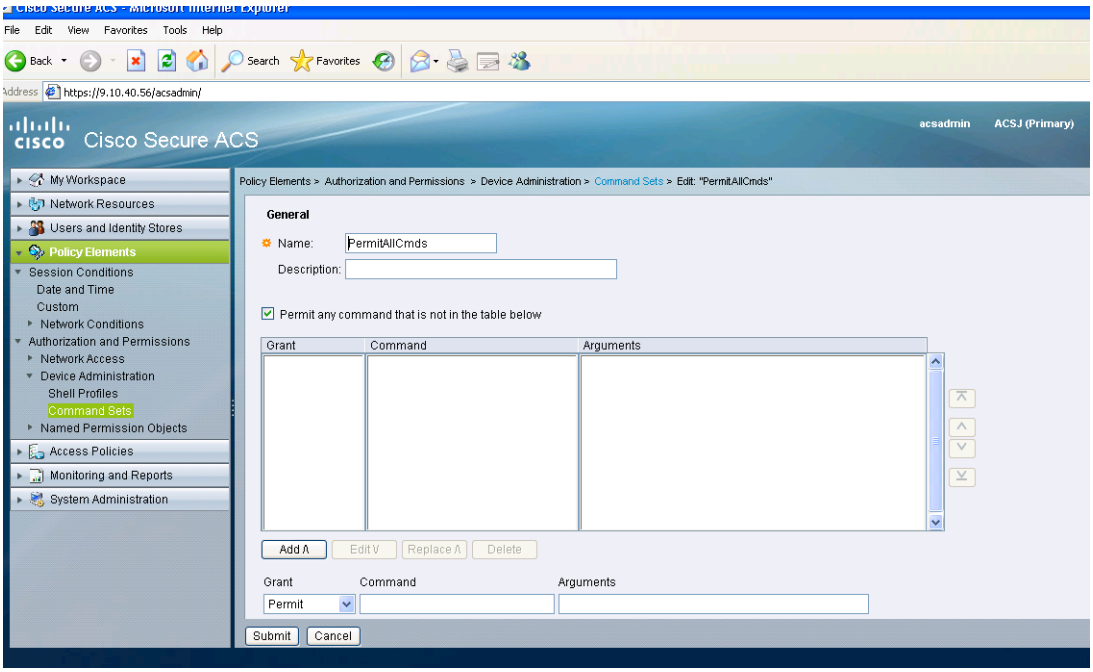
Создайте новый.

Войдите во вкладку "Common Tasks" и установите и максимальные уровни привилегий по умолчанию в 15.



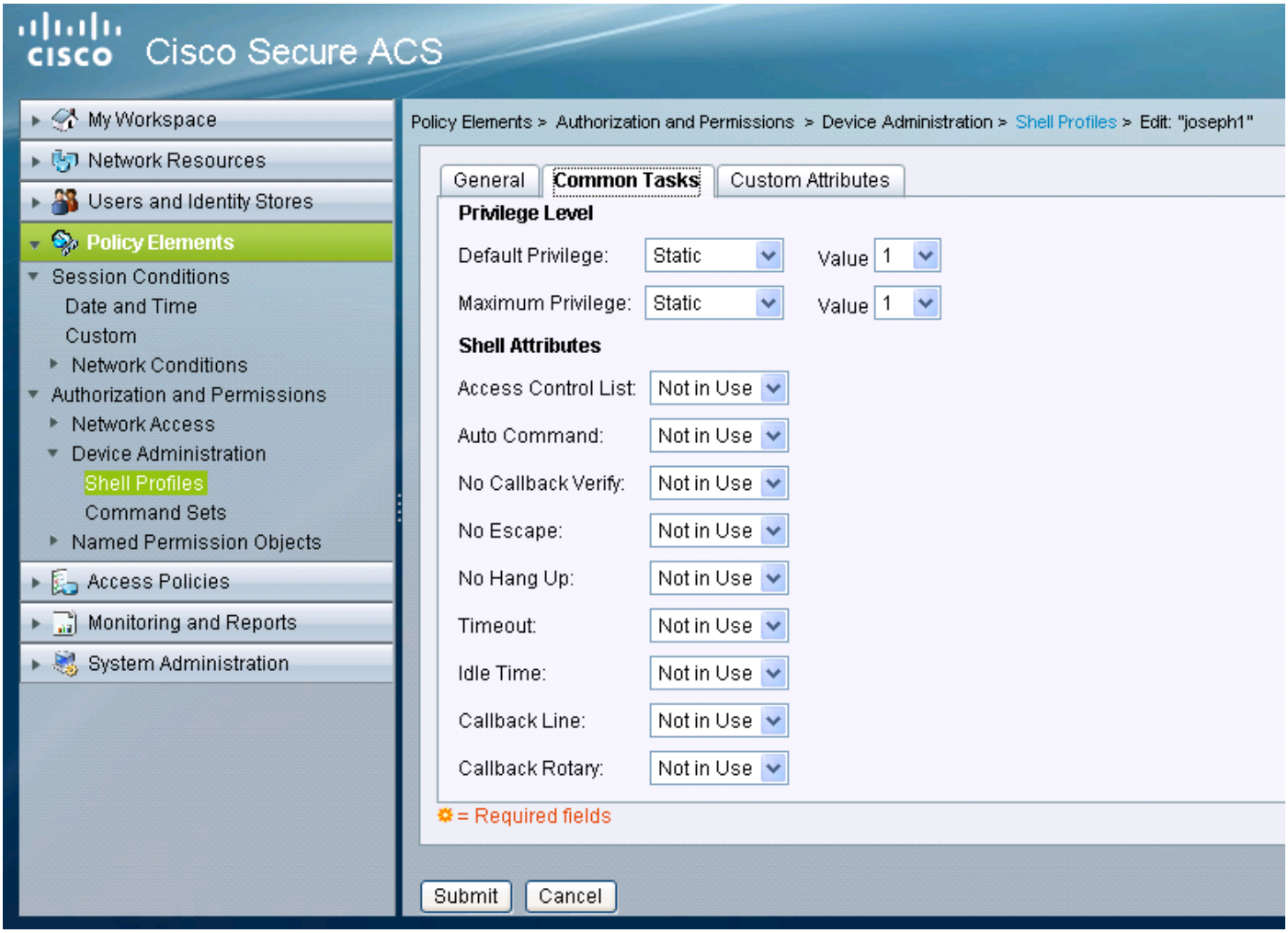
Создание наборов команд для пользователя с правами администратора

Наборы команд являются наборами команд, используемых всеми устройствами tacacs. Они могут использоваться для ограничения команд, которые пользователю разрешают использовать, если назначено что определенный профиль. С тех пор на этих 5760, ограничение сделано на коде Webui на основе уровня привилегий, который передают, наборы команд и для привилегии level1 и для 15 являются тем же.



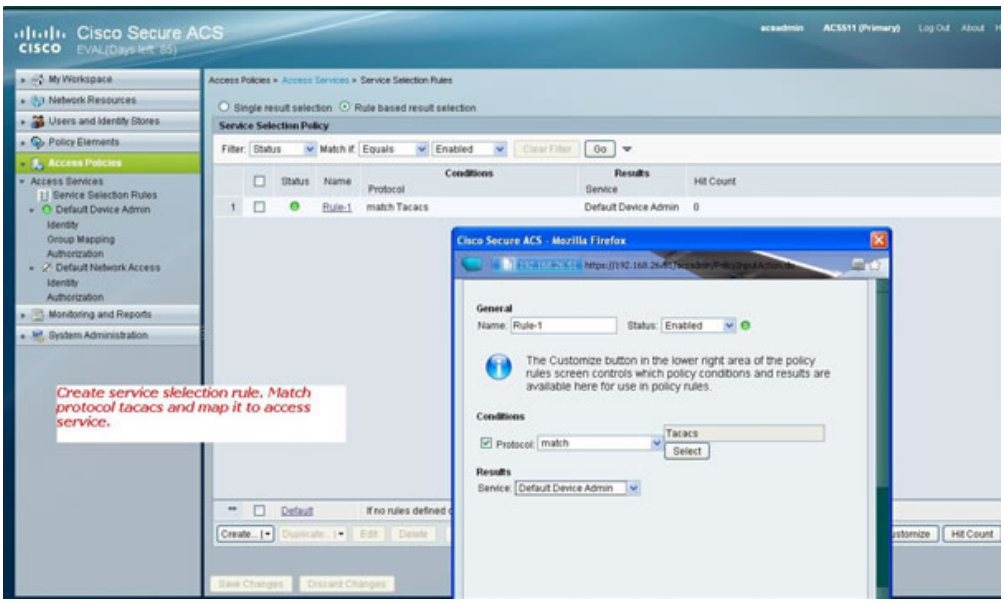
Создание оболочки представляет для пользователя только для чтения

Создайте другой профиль оболочки для пользователей только для чтения. Этот профиль будет отличаться фактом, уровни привилегий установлены в 1.



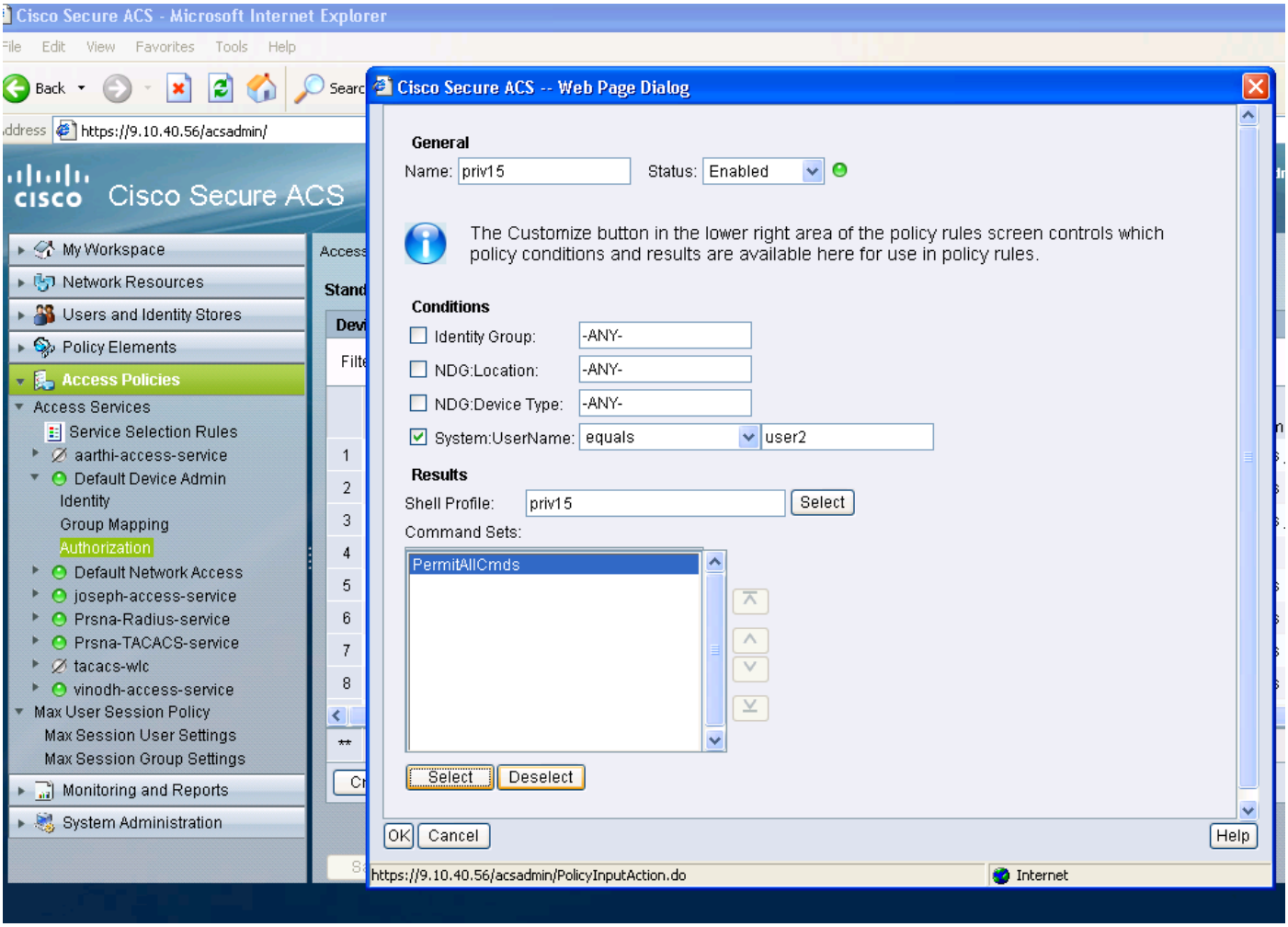
Создайте сервисное правило выбора для соответствия с протоколом tacacs

В зависимости от вашей политики и конфигурации, удостоверьтесь, что у вас есть правило соответствующий tacacs, прибывающий из 5760.



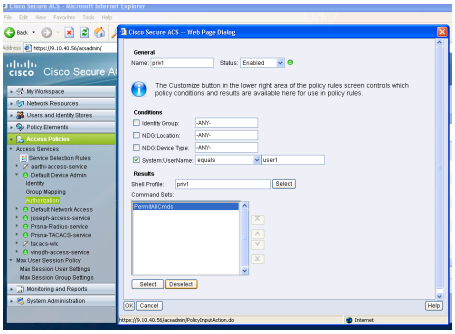
Создайте политику авторизации для полного административного доступа.

Политика Администратора устройства по умолчанию, используемая с выбором протокола tacacs, выбрана как часть процесса политики оценки. При использовании протокола tacacs для аутентификации выбранную политику обслуживания называют политикой Администратора устройства по умолчанию. Та политика сам по себе включает 2 раздела. Identiy имеет в виду, кто пользователь и что делает группа он принадлежит (локальный или внешний) и что ему разрешают сделать согласно настроенному профилю авторизации. Назначьте набор команд, отнесенный на пользователя, которого вы настраиваете.



Создайте политику авторизации для административного доступа только для чтения.

То же сделано для пользователей только для чтения. Данные примеры настраивают уровень привилегий 1 профиль оболочки для пользователя 1 и привилегия 15 пользователю 2.



Настройка 5760 для tacacs

1. Радиус/сервер tacacs должен быть настроен.

сервер tacacs tac_acct

address ipv4 9.1.0.100

ключевой Cisco

1. Настройте группу серверов

aaa group server tacacs+ gtac

имя сервера tac_acct

Нет никакой предпосылки до вышеупомянутого шага.

1. настройте списки методов проверки подлинности и авторизация

aaa authentication login <method-list> группа <srv-группа>

exec aaa authorization <method-list> srv-группа группы>

группа по умолчанию exec aaa authorization <srv-группа> ----Ã обходит для получения tacacs на http.

Вышеупомянутые 3 команды и все другие параметры проверки подлинности и авторизация должны использовать ту же базу данных, или радиус/tacacs или локальные

Например, если для авторизации для выполнения команд нужно к включенному, она также должна указывать на ту же базу данных.

Поскольку исключая:

команды авторизации aaa 15 <method-list> группа <srv-группа> ??> группа серверов, указывающая на базу данных (tacacs/радиус или локальный), должна быть тем же.

1. настройте http для использования вышеупомянутых списков методов

аутентификация входа в систему aaa ip http authentication <method-list> ??? даже если список методов,> списку методов нужно к указанному явно здесь? по умолчанию?

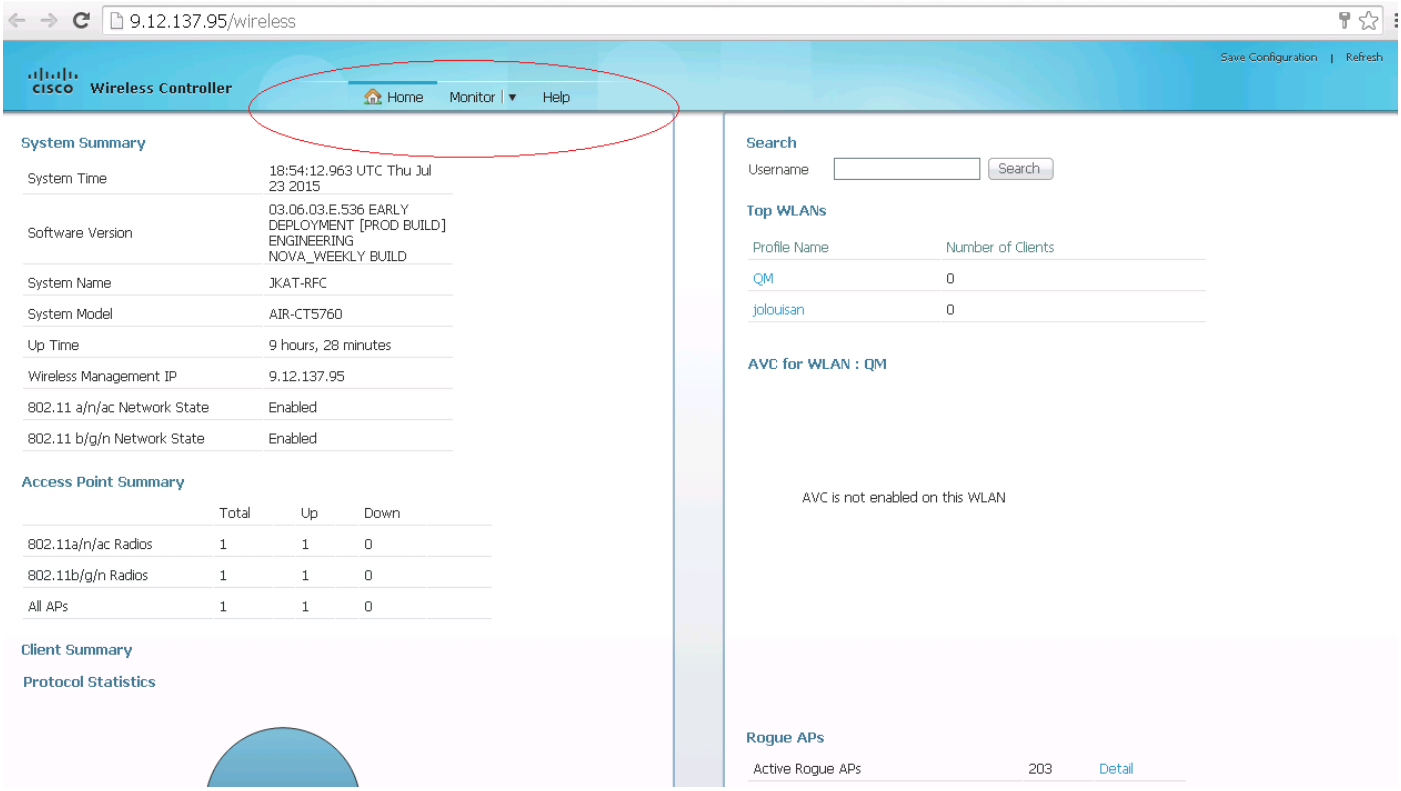
аутентификация exec aaa ip http authentication <method-list>

** Моменты, которые необходимо отметить,

- Не настраивать списки методов на? line vty? параметры конфигурации. Если бы вышеупомянутые шаги и line vty имеют другие конфигурации, то конфигурации line vty имели бы приоритет.
- База данных должна быть тем же через все типы конфигурации управления как ssh/telnet и webui.
- Аутентификации HTTP нужно определить список методов явно.

Доступ к тем же 5760 с 2 другими профилями

Ниже доступ от уровня привилегий 1 пользователь, где предоставляют ограниченному доступу



Ниже доступ от уровня привилегий 15 пользователей, где вы - предоставленный полный доступ