Проверка подлинности "администратора подъезда" контроллера беспроводной сети с помощью сервера RADIUS

Содержание

Введение

Этот документ объясняет действия настройки, включенные для аутентификации администратора лобби контроллера беспроводной локальной сети (WLC) с сервером RADIUS.

Предварительные условия

Требования

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

- Знание того, как настроить основные параметры на WLC
- Знание того, как настроить сервер RADIUS, такой как Cisco Secure ACS
- Знание гостей в WLC

Используемые компоненты

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

- Контроллер беспроводной локальной сети Cisco 4400, который выполняет версию 7.0.216.0
- Cisco Secure ACS, который работает под управлением ПО версии 4.1 и используется в качестве сервера RADIUS в этой конфигурации.

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.

Общие сведения

Администратор лобби, также известный как посол лобби WLC, может создать и управлять учетными записями гостя на Контроллере беспроводной локальной сети (WLC). Посол лобби ограничил привилегии конфигурации и может обратиться, только веб-страницы использовали управлять гостевыми учетными записями. Посол лобби может задать период времени, который считает гость, остаются активными. После того, как заданное время истекает, учетные записи гостя истекают автоматически.

См. Руководство по развертыванию: Гостевой доступ Cisco Использование контроллера беспроводной локальной сети Cisco для получения дополнительной информации о гостях.

Для создания учетной записи гостя на WLC необходимо войти к контроллеру как администратор лобби. Этот документ объясняет, как пользователь аутентифицируется в WLC как администратор лобби на основе атрибутов, возвращенных сервером RADIUS.

Примечание: Проверка подлинности администратора лобби может также быть выполнена на основе учетной записи администратора лобби, настроенной локально на WLC. См. Создание Учетной записи Посла Лобби на информацию того, как создать учетную запись администратора лобби локально на контроллере.

Настройка

В этом разделе вам предоставляют информацию о том, как настроить WLC и Cisco Secure ACS для цели, описанной в этом документе.

Конфигурации

Эти конфигурации используются в данном документе:

- IP-адрес Интерфейса управления WLC является 10.77.244.212/27.
- IP-адрес сервера RADIUS является 10.77.244.197/27.
- Общий секретный ключ, который используется на точке доступа (AP) и сервере RADIUS, является cisco123.
- Имя пользователя и пароль администратора лобби, настроенного в сервере RADIUS,

оба lobbyadmin.

В примере конфигурации в этом документе любому пользователю, входящему в контроллер с именем пользователя и паролем как lobbyadmin, назначают роль администратора лобби.

Настройка WLC

Прежде чем вы запустите необходимую конфигурацию WLC, гарантируете, что ваш контроллер выполняет версию 4.0.206.0 или позже. Это происходит из-за идентификатора ошибки Cisco CSCsg89868 (только зарегистрированные клиенты), в которых веб-интерфейс контроллера отображает неправильные веб-страницы для пользователя LobbyAdmin, когда имя пользователя сохранено в Базе данных RADIUS. LobbyAdmin предоставляют интерфейс ReadOnly вместо интерфейса LobbyAdmin.

Этот дефект был решен в версии 4.0.206.0 WLC. Поэтому гарантируйте, что ваша версия контроллера 4.0.206.0 или позже. См. Обновление программного обеспечения Контроллера беспроводной локальной сети (WLC) для инструкций по тому, как обновить ваш контроллер к соответствующей версии.

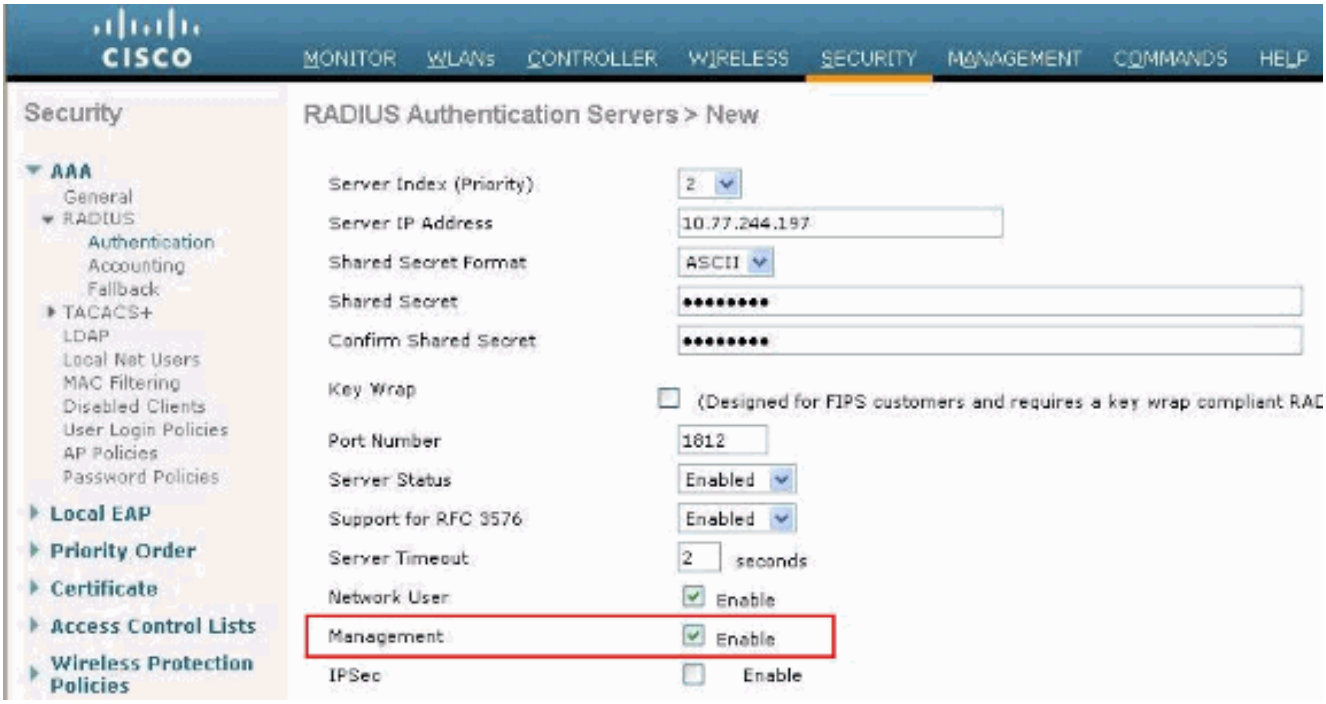
Для выполнения аутентификации управления контроллера с сервером RADIUS гарантируйте, что **флаг Admin-auth-via-RADIUS** включен на контроллере. Это может быть проверено от выходных данных **команды show radius summary**.

Первый шаг должен настроить информацию о сервере RADIUS о контроллере и установить достижимость Уровня 3 между контроллером и сервером RADIUS.

Настройте информацию о сервере RADIUS о контроллере

Выполните эти шаги для настройки WLC с подробными данными о ACS:

1. От GUI WLC выберите **Вкладку Безопасность** и настройте IP-адрес и общий секретный ключ сервера ACS.Этот общий секретный ключ должен быть тем же на ACS для WLC для передачи с ACS.**Примечание:** Общий секретный ключ ACS учитывает регистр. Поэтому удостоверьтесь, что ввели информацию об общем секретном ключе правильно.Эти данные показывают
   пример:



2. Проверьте флажок **Management**, чтобы позволить ACS управлять пользователями WLC как показано на рисунке в шаге 1. **Затем нажмите Apply.**
3. Проверьте достижимость Уровня 3 между контроллером и настроенным сервером RADIUS с помощью **команды ping**. Эта опция ping также доступна на странице настроенного сервера RADIUS в GUI WLC во вкладке **Security> RADIUS Authentication**.Эта схема показывает ответ успешного завершения команды ping от сервера RADIUS. Поэтому достижимость Уровня 3 доступна между контроллером и сервером
RADIUS.

Конфигурация сервера RADIUS

Выполните шаги в этих разделах для настройки сервера RADIUS:

1. Добавьте WLC как клиента AAA к серверу RADIUS
2. Настройте соответствующий атрибут Service-Type IETF RADIUS для администратора лобби

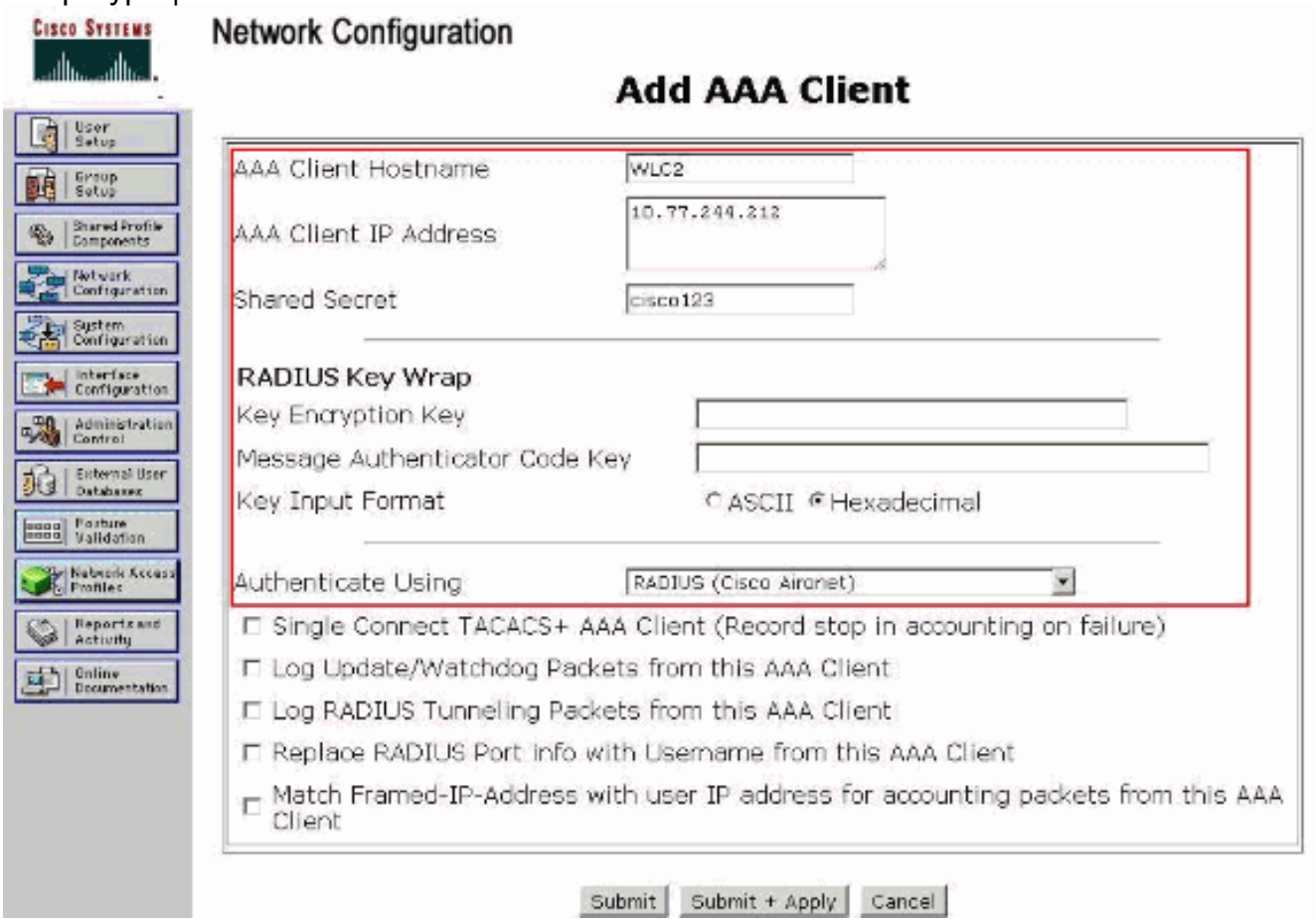
Добавьте WLC как клиента AAA к серверу RADIUS

Выполните эти шаги для добавления WLC как клиент AAA в сервере RADIUS. Как

отмечалось ранее, этот документ использует ACS в качестве сервера RADIUS. Можно использовать любой сервер RADIUS для этой конфигурации.

Выполните эти шаги для добавления WLC как клиент AAA в ACS:

1. От GUI ACS выберите вкладку **Network Configuration**.
2. **На вкладке AAA Clients (Клиенты AAA) щелкните Add Entry (Добавить запись).**
3. В окне Add AAA Client введите имя хоста WLC, IP-адрес WLC и общий секретный ключ. См. схему в качестве примера при шаге 5.
4. От раскрывающегося меню Используемой аутентификации выберите **RADIUS (Cisco Aironet)**.
5. Нажмите **Submit + Перезапуск** для сохранения конфигурации.



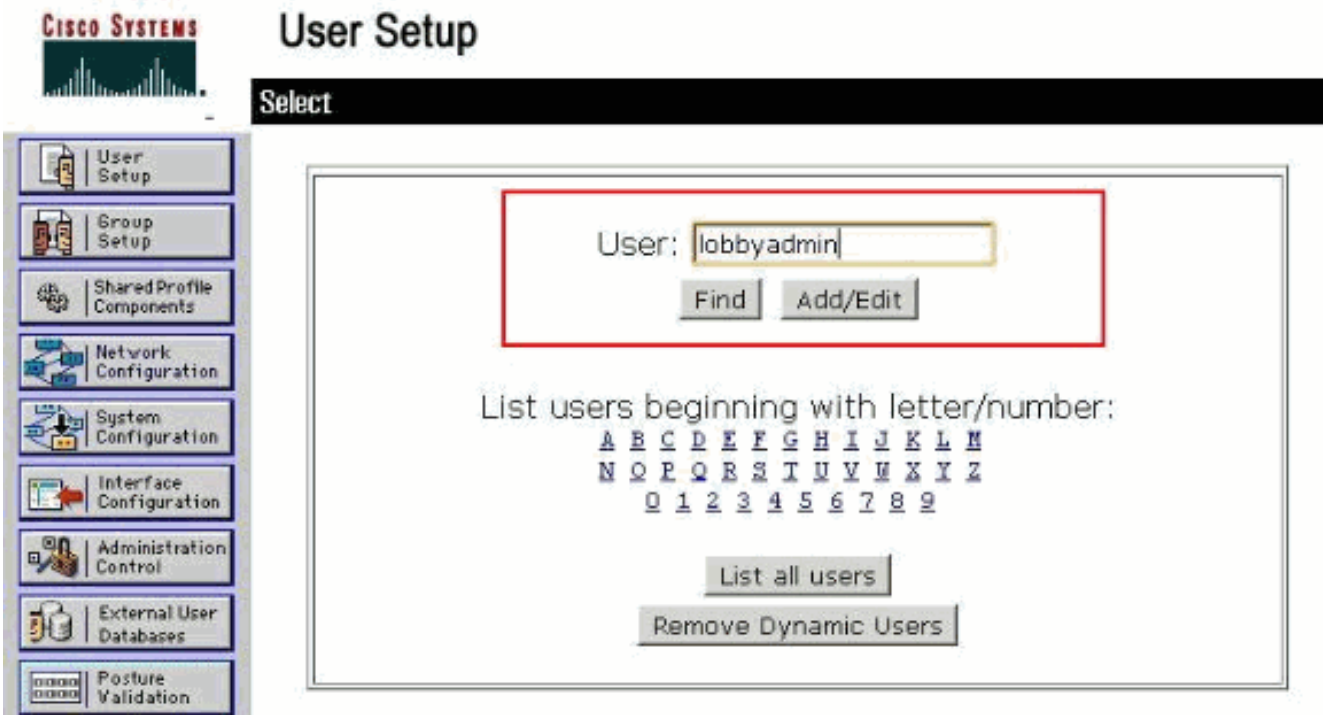
Настройте соответствующий атрибут Service-Type IETF RADIUS для администратора лобби

Для аутентификации пользовательского интерфейса управления контроллера как администратор лобби через сервер RADIUS необходимо добавить, что пользователь к Базе данных RADIUS с Service-Type РАДИУСА IETF приписывает набор **Административному Обратному вызову**. Этот атрибут назначает определенного пользователя роль администратора лобби на контроллере.

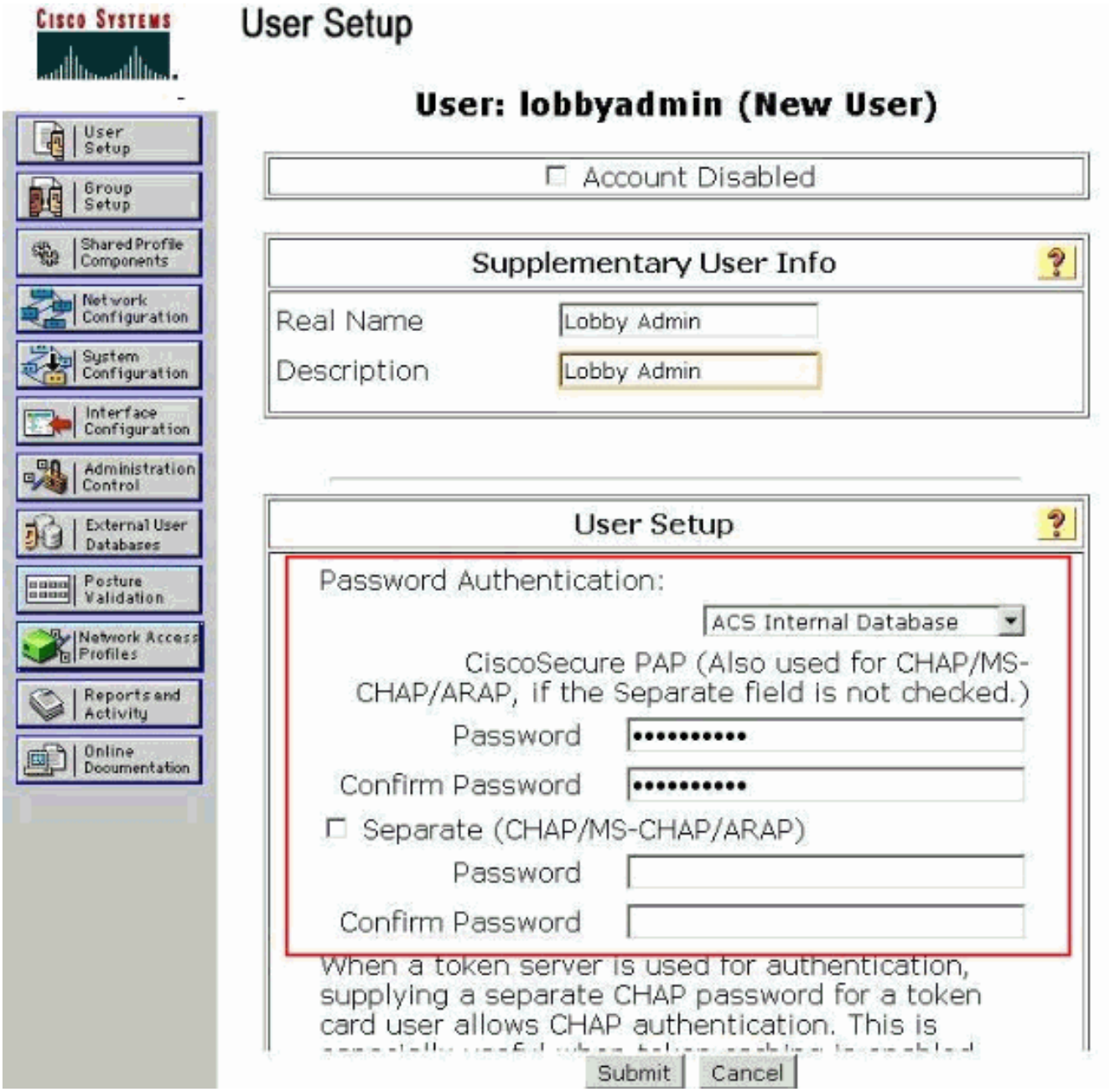
Этот документ показывает пользователю в качестве примера lobbyadmin как администратор лобби. Для настройки этого пользователя выполните эти шаги на ACS:

1. От GUI ACS выберите вкладку **User Setup**.
2. Введите имя пользователя, которое будет добавлено к ACS, поскольку окно данного

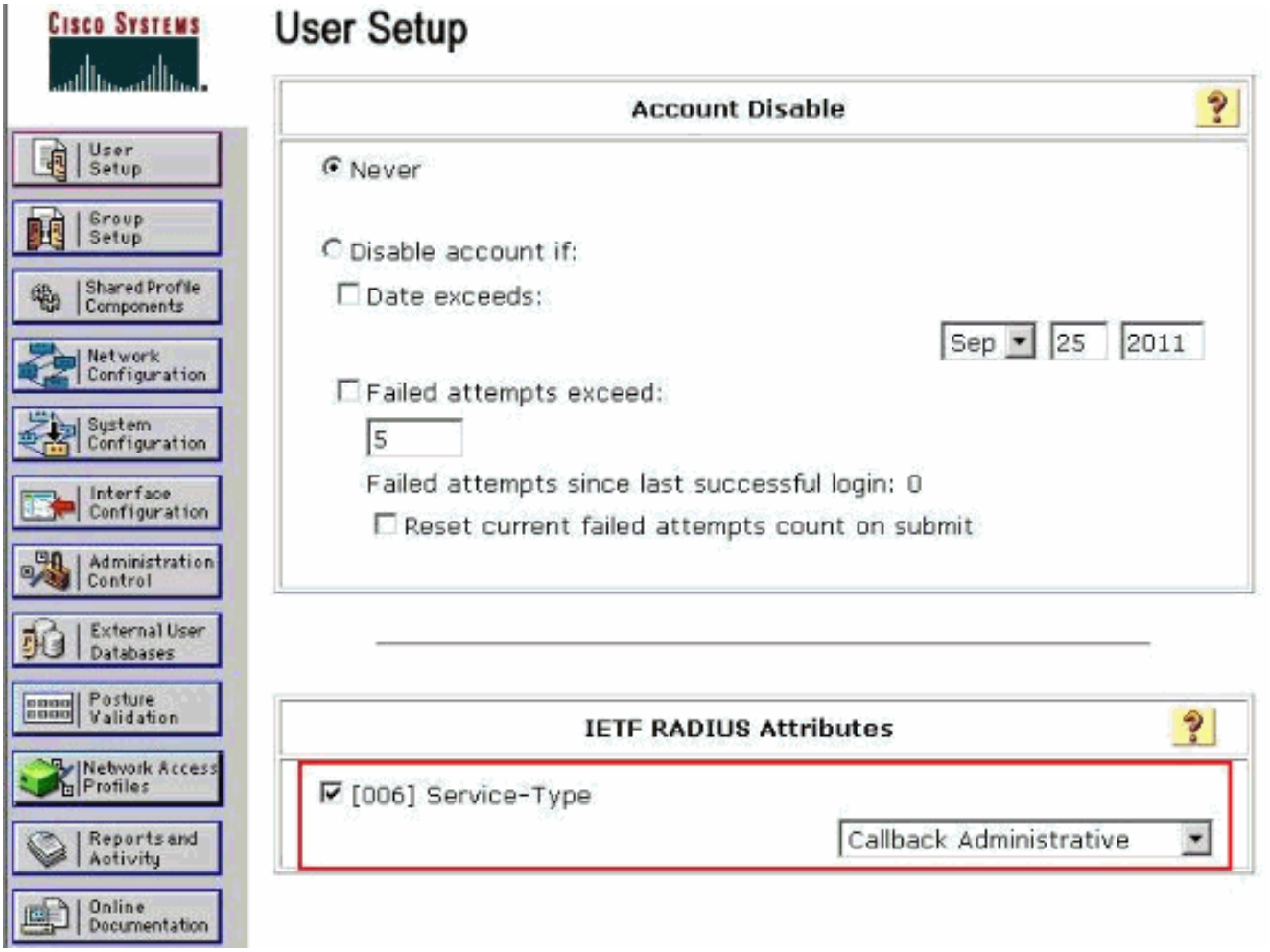
примера
показывает:



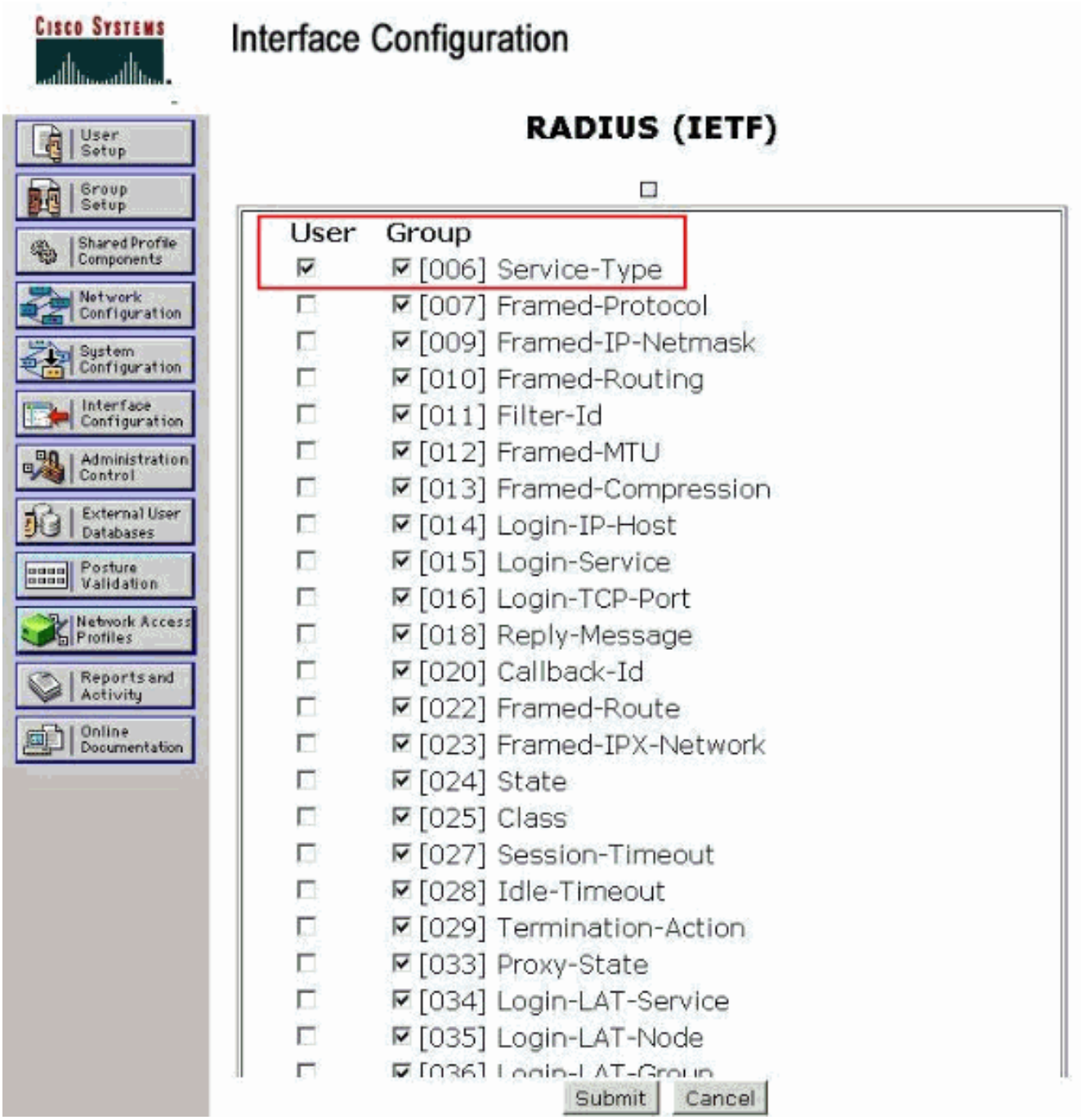
3. Нажмите **Add/Edit**, чтобы перейти к Пользовательской странице Edit.
4. На Пользовательской странице Edit предоставьте Настоящее имя, Описание и подробные данные Пароля этого пользователя.В данном примере используемое имя пользователя и пароль оба
lobbyadmin.



5. Прокрутите вниз к значению Атрибутов RADIUS, стандартизированный IETF и проверьте флажок **Service-Type Attribute**.
6. Выберите **Callback Administrative** из ниспадающего меню Service-Type и нажмите **Submit**.Это - атрибут, который назначает этого пользователя роль администратора лобби.



Иногда, этот атрибут Service-Type не видим при параметрах пользователя. В таких случаях выполните эти шаги для создания его видимым:От GUI ACS выберите **Interface Configuration> RADIUS (IETF)** для включения атрибутов IETF в окне User Configuration.Это приносит вам к RADIUS (IETF) Страница настроек.От RADIUS (IETF) Страница настроек можно включить атрибут IETF, который должен быть видим при пользователе или параметрах группы. Для этой конфигурации проверьте **Service-Type** для Столбца пользователь и нажмите **Submit**.Это окно показывает пример:



Примечание: Данный пример задает аутентификацию на основе для каждого пользователя. Можно также выполнить аутентификацию на основе группы, которой принадлежит индивидуальный пользователь. В таких случаях установите флажок **Флажка Группа** так, чтобы этот атрибут был видим при Параметрах группы.**Примечание:** Кроме того, если аутентификация находится на основе группы, необходимо назначить пользователей на конкретную группу и настроить атрибуты IETF параметра группы для обеспечения привилегий доступа пользователям той группы. См. менеджмент Группы пользователей для получения дальнейшей информации о том, как настроить и управлять группами.

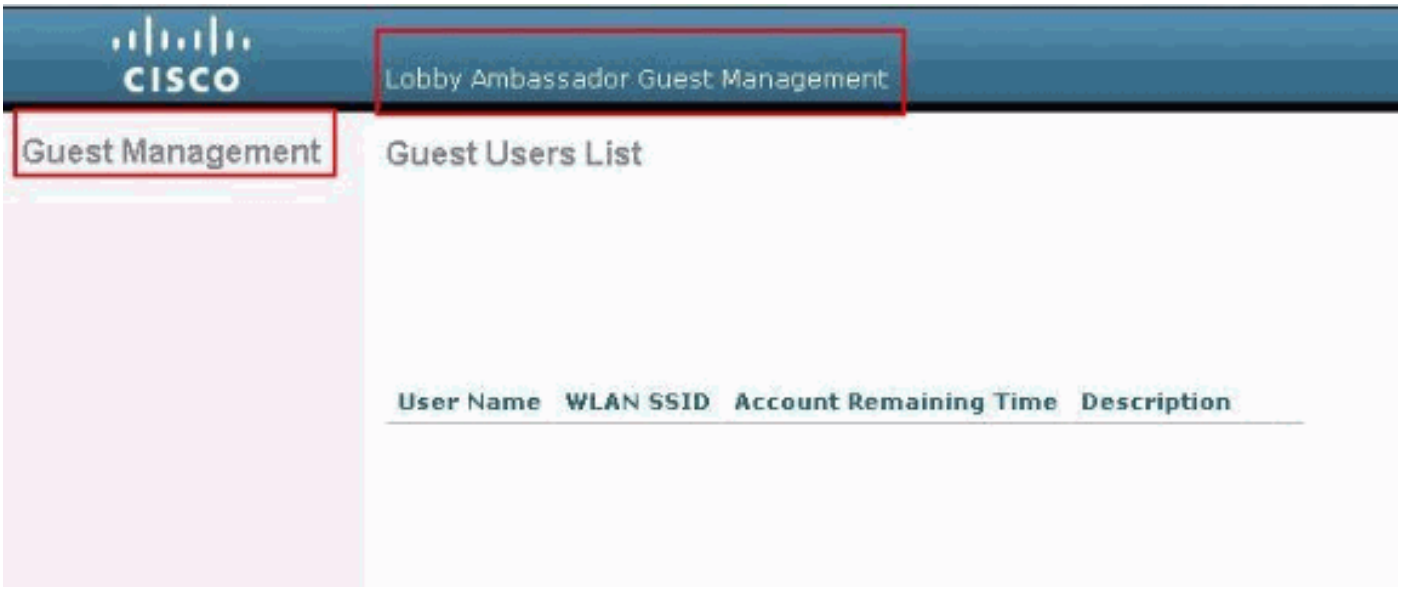
Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Чтобы проверить, что ваша конфигурация работает должным образом, обратитесь к WLC через GUI (HTTP/HTTPS) режим.

Примечание: Посол лобби не может обратиться к CLI - интерфейсу контроллера и поэтому может создать учетные записи гостя только от графического интерфейса контроллера.

Когда приглашение регистрации появится, введите имя пользователя и пароль согласно конфигурации в ACS. Если у вас есть корректные конфигурации, вы аутентифицируетесь успешно в WLC как **администратор лобби**. Данный пример показывает, как GUI администратора лобби заботится об успешной аутентификации:



Примечание: Вы видите, что у администратора лобби нет никакой другой опции кроме управления гостя.

Для проверки его от режима интерфейса командой строки, Telnet в контроллер как администратор чтения-записи. Выполните **команду debug aaa all enable** в CLI контроллера.

```
(Cisco Controller) >debug aaa all enable (Cisco Controller) > *aaaQueueReader: Aug 26
18:07:35.072: ReProcessAuthentication previous proto 28, next proto 20001 *aaaQueueReader: Aug
26 18:07:35.072: AuthenticationRequest: 0x3081f7dc *aaaQueueReader: Aug 26 18:07:35.072:
Callback.....0x10756dd0 *aaaQueueReader: Aug 26 18:07:35.072:
protocolType.....0x00020001 *aaaQueueReader: Aug 26 18:07:35.072:
proxyState.....00:00:00:40: 00:00-00:00 *aaaQueueReader: Aug 26
18:07:35.072: Packet contains 5 AVPs (not shown) *aaaQueueReader: Aug 26 18:07:35.072:
apfVapRadiusInfoGet: WLAN(0) dynamic int attributes srcAddr: 0x0, gw:0x0, mask:0x0, vlan:0,
dpPort:0, srcPort:0 *aaaQueueReader: Aug 26 18:07:35.073: 00:00:00:40:00:00 Successful
transmission of Authentication Packet (id 39) to 10.77.244.212:1812, proxy state
00:00:00:40:00:00-00:01 *aaaQueueReader: Aug 26 18:07:35.073: 00000000: 01 27 00 47 00 00 00 00
00 00 00 00 00 00 00 00 .'.G..... *aaaQueueReader: Aug 26 18:07:35.073: 00000010: 00 00
00 00 01 0c 6c 6f 62 62 79 61 64 6d 69 6e ......lobbyadmin *aaaQueueReader: Aug 26 18:07:35.073:
00000020: 02 12 5f 5b 5c 12 c5 c8 52 d3 3f 4f 4f 8e 9d 38 .._[\...R.?OO..8 *aaaQueueReader: Aug
26 18:07:35.073: 00000030: 42 91 06 06 00 00 00 07 04 06 0a 4e b1 1a 20 09 B.....N....
*aaaQueueReader: Aug 26 18:07:35.073: 00000040: 57 4c 43 34 34 30 30 WLC4400
*radiusTransportThread: Aug 26 18:07:35.080: 00000000: 02 27 00 40 7e 04 6d 533d ed 79 9c b6 99
d1 f8 .'.@~.mS=.y..... *radiusTransportThread: Aug 26 18:07:35.080: 00000010: d0 5a 8f 4f 08 06
ff ffff ff 06 06 00 00 00 0b .Z.O..... *radiusTransportThread: Aug 26 18:07:35.080:
00000020: 19 20 43 41 43 53 3a 302f 61 65 32 36 2f 61 34 ..CACS:0/ae26/a4
*radiusTransportThread: Aug 26 18:07:35.080: 00000030: 65 62 31 31 61 2f 6c 6f62 62 79 61 64 6d
69 6e eb11a/lobbyadmin *radiusTransportThread: Aug 26 18:07:35.080: ****Enter
processIncomingMessages: response code=2 *radiusTransportThread: Aug 26 18:07:35.080: ****Enter
processRadiusResponse: response code=2 *radiusTransportThread: Aug 26 18:07:35.080:
```

```
00:00:00:40:00:00 Access-Accept received from RADIUS server 10.77.244.212 for mobile
00:00:00:40:00:00 receiveId = 0 *radiusTransportThread: Aug 26 18:07:35.080:
AuthorizationResponse: 0x13c73d50 *radiusTransportThread: Aug 26 18:07:35.080:
structureSize.............................118 *radiusTransportThread: Aug 26 18:07:35.080:
resultCode.................................0 *radiusTransportThread: Aug 26 18:07:35.080:
protocolUsed.............................0x00000001 *radiusTransportThread: Aug 26
18:07:35.080: proxyState.................................00:00:00:40:00:00-00:00
*radiusTransportThread: Aug 26 18:07:35.080: Packet contains 3 AVPs: *radiusTransportThread: Aug
26 18:07:35.080: AVP[01] Framed-IP-Address.....................0xffffffff (-1) (4 bytes)
*radiusTransportThread: Aug 26 18:07:35.080: AVP[02] Service-
Type.............................0x0000000b (11) (4 bytes) *radiusTransportThread: Aug 26
18:07:35.080: AVP[03] Class..................................... CACS:0/ae26/a4eb11a/lobbyadmin
(30 bytes) *emWeb: Aug 26 18:07:35.084: Authentication succeeded for lobbyadmin
```

В выделенной информации в этих выходных данных вы видите, что service-type приписывает 11 (Административный Обратный вызов) передан на контроллер от сервера ACS, и в пользователя входят как администратор лобби.

Эти команды могли бы иметь дополнительную справку:

- **подробные данные debug aaa включают**
- **debug aaa events enable**
- **debug aaa packets enable**

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Устранение неполадок

Когда вы входите к контроллеру с послом лобби привилегии, вы не в состоянии создать учетную запись гостя с **"0"** пожизненное значение, которое является учетной записью, которая никогда не истекает. В этих ситуациях вы получаете сообщение об ошибках `Lifetime value cannot be 0`.

Это происходит из-за идентификатора ошибки Cisco CSCsf32392 (только зарегистрированные клиенты), который найден в основном с версией 4.0 WLC. Этот дефект был решен в версии 4.1 WLC.

Дополнительные сведения

- Пример конфигурации проверки сервером RADIUS подлинности административных пользователей на контроллере
- Конфигурация единой беспроводной сети Cisco TACACS+
- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 4.0 - управляющие учетные записи пользователя
- Пример конфигурации ACL на контроллере беспроводных LAN
- Часто задаваемые вопросы по контроллеру беспроводной LAN (WLC)
- ACL на контроллерах беспроводных LAN: "Правила, ограничения и примеры"
- Пример настройки контроллера беспроводной сети с внешней веб-аутентификацией
- Пример настройки веб-аутентификации контроллера беспроводной LAN
- Пример настройки гостевой беспроводной локальной сети (WLAN) и внутренней беспроводной локальной сети при использовании контроллеров беспроводных локальных сетей (WLC)

- Cisco Systems – техническая поддержка и документация