

Конфигурация единой беспроводной сети Cisco TACACS+

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[TACACS + реализация в контроллере](#)

[Authentication](#)

[Authorization](#)

[Учет](#)

[TACACS + конфигурация в WLC](#)

[Добавьте TACACS + сервер проверки подлинности](#)

[Добавьте TACACS + сервер авторизации](#)

[Добавьте TACACS + учетный сервер](#)

[Настройте заказ аутентификации](#)

[Проверка конфигурации](#)

[Настройте сервер Cisco Secure ACS](#)

[Конфигурация сети](#)

[Настройка интерфейса](#)

[User/Group Setup](#)

[Учетные записи в Cisco Secure ACS](#)

[TACACS + конфигурация в WCS](#)

[WCS с помощью виртуальных доменов](#)

[Настройте Cisco Secure ACS для использования WCS](#)

[Конфигурация сети](#)

[Настройка интерфейса](#)

[User/Group Setup](#)

[Отладка](#)

[Отладки от WLC для role1=ALL](#)

[Отладки от WLC для множественных ролей](#)

[Отладки от WLC для сбоя авторизации](#)

[Дополнительные сведения](#)

Введение

Этот документ содержит пример конфигурации системы TACACS на контроллере беспроводной локальной сети Cisco (WLC) и системы управления беспроводной сетью

Cisco (WCS) для унифицированной беспроводной сети Cisco. Этот документ также дает ряд советов по устранению основных видов неисправностей.

TACACS + является протоколом клиент/сервер, который предоставляет централизованную защиту для пользователей, которые пытаются получить управляющего доступ к маршрутизатору или серверу доступа к сети. TACACS + предоставляет эти сервисы AAA:

- Аутентификация пользователей, пытающихся войти к сетевому оборудованию
- Авторизация определить то, что должен иметь уровень пользователей доступа
- При учете для отслеживания все изменения пользователь делает

См. [TACACS Настройки +](#) для получения дополнительной информации о сервисах AAA и TACACS + функциональность.

См. [TACACS + и Сравнение RADIUS](#) для сравнения TACACS + и RADIUS.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Знание того, как настроить WLC и облегченные точки доступа (LAP) для главной операции
- Знание Протокола LWAPP и методов безопасности беспроводной связи
- RADIUS базовых знаний и TACACS +
- Базовые знания о конфигурации AcS Cisco

Используемые компоненты

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

- Cisco Secure ACS для Версии Windows 4.0
- Контроллер беспроводной локальной сети Cisco, который выполняет версию 4.1.171.0. TACACS + функциональность на WLC поддерживается на версии программного обеспечения 4.1.171.0 или позже.
- Cisco Wireless Control System, который выполняет версию 4.1.83.0. TACACS + функциональность на WCS поддерживается на версии программного обеспечения 4.1.83.0 или позже.

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.](#)

TACACS + реализация в контроллере

Authentication

Аутентификация может быть выполнена с помощью локальной базы данных, RADIUS или TACACS + сервер, который использует имя пользователя и пароль. Реализация не является полностью модульной. Сервисы проверки подлинности и авторизация связаны друг к другу. Например, если аутентификация выполнена с помощью RADIUS/локальной базы данных, то авторизация не выполнена с TACACS +. Это использовало бы разрешения, привязанные для пользователя в локальной переменной или Базе данных RADIUS, такой как только для чтения или чтение-запись, тогда как, когда аутентификация выполнена с TACACS +, авторизация связана к TACACS +.

В случаях, где несколько баз данных настроены, CLI предоставлен для диктовки последовательности, в которой должна быть отнесена база данных бэкэнда.

Authorization

Авторизация является основанной задачей, а не фактическая базирующаяся авторизация на команду. Задачи сопоставлены с различными вкладками, которые соответствуют семи пунктам строки меню, которые в настоящее время находятся на веб-GUI. Это пункты строки меню:

- МОНИТОР
- WLANS
- CONTROLLER
- WIRELESS
- Безопасность
- МЕНЕДЖМЕНТ
- Команда

Причина для этого сопоставления основывается на факте, что большинство клиентов использует веб-интерфейс для настройки контроллера вместо CLI.

Дополнительная роль для управления admin лобби (LOBBY) доступна пользователям, которые должны иметь административные привилегии лобби только.

Задача, что пользователь назван, настроена в TACACS + (ACS) сервер с помощью пользовательских пар атрибут-значение (AV). Пользователь может авторизоваться для одного или множественных задач. Минимальная авторизация является МОНИТОРОМ только, и максимумом является ALL (авторизовавший выполнить все семь вкладок). Если пользователь не назван для определенной задачи, пользователю все еще разрешают обратиться к той задаче в режиме чтения. Если аутентификация включена, и сервер проверки подлинности становится недостижимым или неспособным авторизовать, пользователь не может войти к контроллеру.

Примечание: Для аутентификации основных функций управления через TACACS + для следования необходимо настроить серверы проверки подлинности и авторизация на WLC. Бухгалтерская конфигурация является дополнительной.

Учет

Учет происходит каждый раз, когда инициируемое индивидуальными пользователями действие выполнено успешно. Измененные атрибуты зарегистрированы в TACACS + учетный сервер наряду с ними:

- Идентификатор пользователя частного лица, которое внесло изменение
- Удаленный хост от того, где входят в пользователя
- Дата и время, когда была выполнена команда
- Уровень авторизации пользователя
- Предоставлена строка, которая предоставляет сведения относительно того, какое действие было выполнено и значения,

Если учетный сервер становится недостижимым, пользователь может все еще продолжить сеанс.

Примечание: Учетные записи не генерируются от WCS в выпуске ПО 4.1 или earlier.

[TACACS + конфигурация в WLC](#)

Выпуск 4.1.171.0 Программного обеспечения WLC и позже представляет новые CLI и веб-изменения GUI для включения TACACS + функциональность на WLC. Представленные CLI перечислены в этом разделе для ссылки. Соответствующие изменения к веб-GUI добавлены под Вкладкой Безопасность.

Этот документ предполагает, что уже завершена базовая конфигурация WLC.

Для настройки TACACS + в контроллере WLC, необходимо выполнить эти шаги:

1. [Добавьте TACACS + сервер проверки подлинности](#)
2. [Добавьте TACACS + сервер авторизации](#)
3. [Добавьте TACACS + учетный сервер](#)
4. [Настройте заказ аутентификации](#)

[Добавьте TACACS + сервер проверки подлинности](#)

Выполните эти шаги для добавления TACACS + Сервер проверки подлинности:

1. Используйте GUI и перейдите к **Безопасности> TACACS +> Аутентификация**.



2. Добавьте IP-адрес TACACS + сервер и введите общий секретный ключ. При необходимости измените порт по умолчанию

TCP/49.

The screenshot shows the Cisco configuration interface for TACACS+ Authentication Servers. The left sidebar is under 'Security' with 'TACACS+' expanded. The main area is titled 'TACACS+ Authentication Servers > New'. The configuration fields are: Server Index (Priority) set to 1; Server IP Address set to 10.1.1.12; Shared Secret Format set to ASCII; Shared Secret and Confirm Shared Secret fields are masked with asterisks; Port Number set to 49; Server Status set to Enabled; and Retransmit Timeout set to 2 seconds. There are '< Back' and 'Apply' buttons at the top right.

- Щелкните "Применить". Можно выполнить, это от CLI с помощью `config tacacs auth` добавляет `<Индекс Сервера> адрес <IP> <port> [ascii/hex] команда <secret>`: (Cisco Controller) `>config tacacs auth add 1 10.1.1.12 49 ascii cisco123`

[Добавьте TACACS + сервер авторизации](#)

Выполните эти шаги для добавления TACACS + Сервер авторизации:

- От GUI перейдите к **Безопасности > TACACS + > Авторизация**.
- Добавьте IP-адрес TACACS + сервер и введите общий секретный ключ. При необходимости измените порт по умолчанию TCP/49.

The screenshot shows the Cisco configuration interface for TACACS+ Authorization Servers. The left sidebar is under 'Security' with 'TACACS+' expanded. The main area is titled 'TACACS+ Authorization Servers > New'. The configuration fields are: Server Index (Priority) set to 1; Server IP Address set to 10.1.1.12; Shared Secret Format set to ASCII; Shared Secret and Confirm Shared Secret fields are masked with asterisks; Port Number set to 49; Server Status set to Enabled; and Retransmit Timeout set to 2 seconds. There are '< Back' and 'Apply' buttons at the top right.

- Щелкните "Применить". Можно выполнить, это от CLI с помощью `config tacacs athr` добавляет `<Индекс Сервера> адрес <IP> <port> [ascii/hex] команда <secret>`: (Cisco Controller) `>config tacacs athr add 1 10.1.1.12 49 ascii cisco123`

[Добавьте TACACS + учетный сервер](#)

Выполните эти шаги для добавления TACACS + Учетный сервер:

1. Используйте GUI и перейдите к **Безопасности> TACACS +> Учет**.
2. Добавьте IP-адрес сервера и введите общий секретный ключ. При необходимости измените порт по умолчанию TCP/49.

The screenshot shows the Cisco GUI configuration page for TACACS+ Accounting Servers. The page is titled "TACACS+ Accounting Servers > New" and has a "Back" button and an "Apply" button. The configuration fields are as follows:

Field	Value
Server Index (Priority)	1
Server IP Address	10.1.1.12
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Port Number	49
Server Status	Enabled
Retransmit Timeout	5 seconds

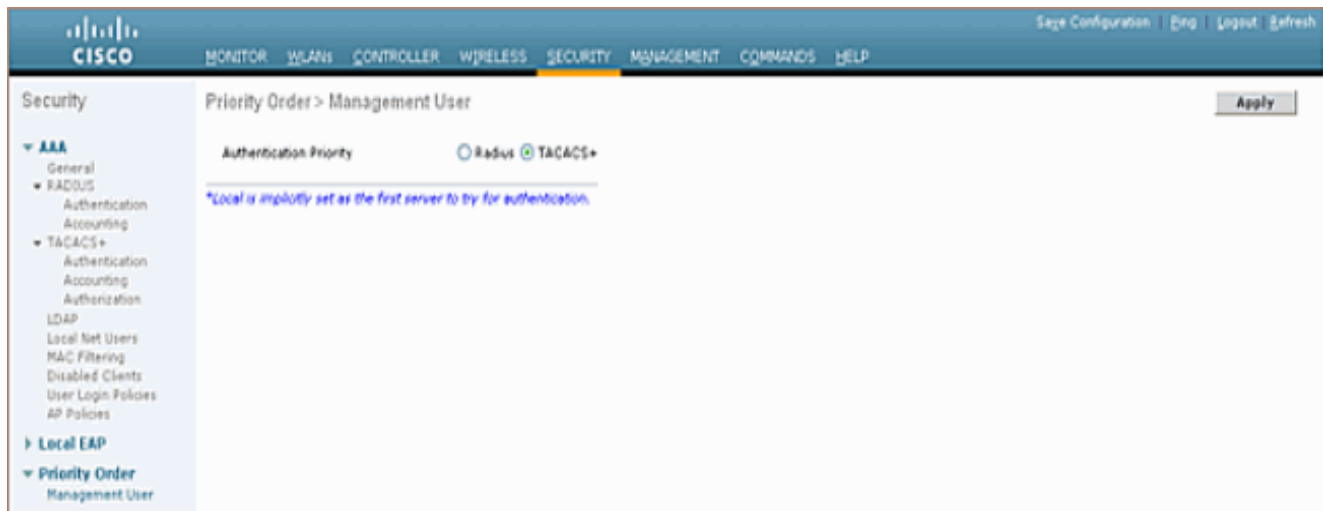
3. Щелкните "Применить". Можно выполнить, это от CLI с помощью `config tacacs acct добавляет <Индекс Сервера> адрес <IP> <port> [ascii/hex] команда <secret>`: (Cisco Controller) `>config tacacs acct add 1 10.1.1.12 49 ascii cisco123`

[Настройте заказ аутентификации](#)

Этот шаг объясняет, как настроить заказ AAA аутентификации, когда существуют настроенные несколько баз данных. Заказ аутентификации может быть **локальной переменной** и **RADIUS**, или **локальной переменной** и **TACACS**. Конфигурация контроллера по умолчанию для заказа аутентификации является **локальной переменной** и **RADIUS**.

Выполните эти шаги для настройки заказа аутентификации:

1. От GUI перейдите к **Безопасности> Порядок приоритетов> Пользовательский интерфейс управления**.
2. Выберите приоритет аутентификации. В данном примере был выбран TACACS +.
3. Нажмите **Apply** для выбора для имени места.



Можно выполнить это от CLI с помощью `config aaa auth mgmt <server1>` команда `<server2>`:(Cisco Controller) `>config aaa auth mgmt tacacs local`

Проверка конфигурации

В этом разделе описываются команды, используемые для проверки TACACS + конфигурация на WLC. Это некоторые **полезные команды show**, которые помогают определять, корректна ли конфигурация:

- **show aaa auth** — Предоставляет сведения о заказе аутентификации.(Cisco Controller) `>show aaa auth Management authentication server order:`

```
1..... local
2..... Tacacs
```
- **show tacacs summary** — Отображает сводку TACACS + сервисы и статистика.(Cisco Controller) `>show tacacs summary Authentication Servers Idx Server Address Port State Tout -`

```
----- 1 10.1.1.12 49 Enabled 2 Authorization Servers Idx
Server Address Port State Tout --- ----- 1 10.1.1.12 49
Enabled 2 Accounting Servers Idx Server Address Port State Tout --- -----
----- 1 10.1.1.12 49 Enabled 2
```
- **stats аутентификации show tacacs** — Отображает TACACS + статистика сервера проверки подлинности.(Cisco Controller) `>show tacacs auth statistics Authentication Servers: Server Index..... 1 Server`

```
Address..... 10.1.1.12 Msg Round Trip
Time..... 0 (1/100 second) First
Requests..... 7 Retry
Requests..... 3 Accept
Responses..... 3 Reject
Responses..... 0 Error
Responses..... 0 Restart
Responses..... 0 Follow
Responses..... 0 GetData
Responses..... 0 Encrypt no secret
Responses..... 0 Challenge Responses..... 0
Malformed Msgs..... 0 Bad Authenticator
Msgs..... 0 Timeout Requests..... 12
Unknowntype Msgs..... 0 Other
Drops..... 0
```
- **show tacacs athr stats** — Отображает TACACS + статистика сервера авторизации.(Cisco Controller) `>show tacacs athr statistics Authorization Servers: Server`

```
Index..... 1 Server
Address..... 10.1.1.12 Msg Round Trip
Time..... 0 (1/100 second) First
Requests..... 3 Retry
```

```

Requests..... 3 Received
Responses..... 3 Authorization Success.....
3 Authorization Failure..... 0 Challenge
Responses..... 0 Malformed Msgs.....
0 Bad Athrenticator Msgs..... 0 Timeout
Requests..... 0 Unknowntype
Msgs..... 0 Other Drops..... 0

```

- **show tacacs acct stats** — Отображает TACACS + статистика учетного сервера. (Cisco Controller) >**show tacacs acct statistics** Accounting Servers: Server


```

Index..... 1 Server
Address..... 10.1.1.12 Msg Round Trip
Time..... 0 (1/100 second) First
Requests..... 133 Retry
Requests..... 0 Accounting
Response..... 0 Accounting Request Success..... 0
Accounting Request Failure..... 0 Malformed
Msgs..... 0 Bad Authenticator Msgs.....
0 Timeout Requests..... 399 Unknowntype
Msgs..... 0 Other Drops..... 0

```

[Настройте сервер Cisco Secure ACS](#)

Этот раздел предоставляет шаги, вовлеченные в TACACS + Сервер ACS, чтобы создать сервисы и настраиваемые атрибуты, и назначить роли на пользователей или группы.

Создание пользователей и группы не объяснено в этом разделе. Предполагается, что пользователи и группы созданы по мере необходимости. См. [Руководство пользователя для Cisco Secure ACS для Windows Server 4.0](#) для получения информации о том, как создать пользователей и группы пользователей.

[Конфигурация сети](#)

Выполните следующее действие:

Добавьте управление IP-адресами Контроллера как клиента AAA с Механизмом аутентификации как TACACS + (Cisco IOS).

CiscoSecure ACS - Microsoft Internet Explorer

Address <http://127.0.0.1:1479/>

Network Configuration

AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
DOBSL12-2	10.22.8.21	TACACS+ (Cisco IOS)

Add Entry Search

AAA Servers

AAA Server Name	AAA Server IP Address	AAA Server Type
wnbu-dt-srvr01	11.11.13.2	CiscoSecure ACS

Add Entry Search

Help

- [Network Device Groups](#)
- [Adding a Network Device Group](#)
- [Editing a Network Device Group](#)
- [Deleting a Network Device Group](#)
- [Searching for Network Devices](#)
- [AAA Clients](#)
- [Adding a AAA Client](#)
- [Editing a AAA Client](#)
- [Deleting a AAA Client](#)
- [AAA Servers](#)
- [Adding a AAA Server](#)
- [Editing a AAA Server](#)
- [Deleting a AAA Server](#)
- [Proxy Distribution Table](#)
- [Adding a Proxy Distribution Table Entry](#)
- [Sorting Proxy Distribution Table Entries](#)
- [Editing a Proxy Distribution Table Entry](#)
- [Deleting a Proxy Distribution Table Entry](#)

Applet appPing started Internet

Настройка интерфейса

Выполните следующие действия:

1. В меню Interface Configuration выберите TACACS + (Cisco IOS) ссылка.
2. Включите **новые сервисы**.
3. Установите флажки **Пользователя** и **Флажка Группа**.
4. Введите **ciscowlc** для Сервиса и **характерный** для Протокола.
5. Включите **Advanced TACACS + функции**.

Address <http://127.0.0.1:1767/> Go Links

CISCO SYSTEMS

Interface Configuration

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Posture Validation

Network Access Profiles

Reports and Activity

Online Documentation

TACACS+ Services ?

User	Group	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	PPP IP
<input type="checkbox"/>	<input type="checkbox"/>	PPP IPX
<input type="checkbox"/>	<input type="checkbox"/>	PPP Multilink
<input type="checkbox"/>	<input type="checkbox"/>	PPP Apple Talk
<input type="checkbox"/>	<input type="checkbox"/>	PPP VPDN
<input type="checkbox"/>	<input type="checkbox"/>	PPP LCP
<input type="checkbox"/>	<input type="checkbox"/>	ARAP
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Shell (exec)
<input type="checkbox"/>	<input type="checkbox"/>	PIX Shell (pixshell)
<input type="checkbox"/>	<input type="checkbox"/>	SLIP

New Services

		Service	Protocol
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="ciscowlc"/>	<input type="text" value="common"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Advanced Configuration Options ?

Advanced TACACS+ Features

Display a Time-of-Day access grid for every TACACS+ service where you can

Submit Cancel

6. Нажмите **Submit** для применения изменений.

User/Group Setup

Выполните следующие действия:

1. Выберите ранее созданного Пользователя/Группу.
2. Перейдите к **TACACS + параметры настройки**.
3. Проверьте флажок, который соответствует *ciscowlc* сервису, который был создан в разделе Конфигурации интерфейса.
4. Проверьте флажок **Настраиваемых атрибутов**.



Group Setup

Jump To Access Restrictions

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Shell Command Authorization Set

- None
 - Assign a Shell Command Authorization Set for any network device
 - Per Group Command Authorization
- Unmatched Cisco IOS commands
- Permit
 - Deny

Command:

Arguments:

Unlisted arguments

- Permit
- Deny

ciscowlc common

Custom attributes

Wireless-WCS HTTP

Custom attributes

IETF RADIUS Attributes

[006] Service-Type

Callback NAS Prompt

Submit

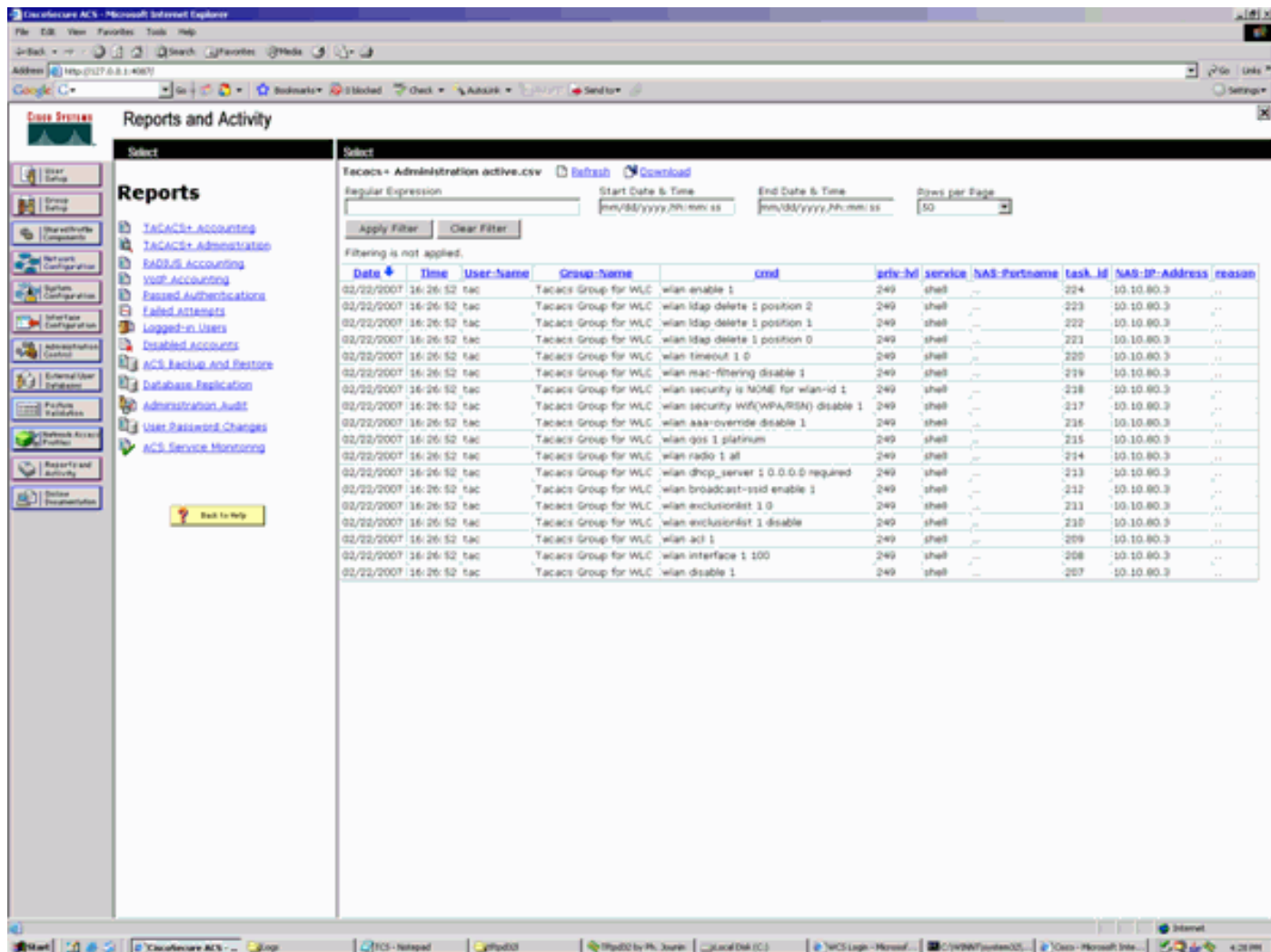
Submit + Restart

Cancel

- В текстовом поле ниже Настраиваемых атрибутов введите этот текст, если пользователь создал доступ потребностей только к WLAN, БЕЗОПАСНОСТИ и КОНТРОЛЛЕРУ: **role1=WLAN role2=SECURITY role3=CONTROLLER**. Если пользователь должен обратиться только к ВКЛАДКЕ БЕЗОПАСНОСТЬ, ввести этот текст: **role1=SECURITY**. Роль соответствует этим семи пунктам строки меню в веб-GUI контроллера. Пункты строки меню являются МОНИТОРОМ, WLAN, КОНТРОЛЛЕРОМ, БЕСПРОВОДНЫМИ СЕТЯМИ, БЕЗОПАСНОСТЬЮ, МЕНЕДЖМЕНТОМ и КОМАНДОЙ.
- Введите роль, в которой пользователь нуждается для role1, role2 и так далее. Если пользователю нужны все роли, то ключевое слово **ALL** должно использоваться. Для роли admin лобби ключевое слово должен использоваться **LOBBY**.

Учетные записи в Cisco Secure ACS

TACACS + учетные записи от WLC доступны в Cisco Secure ACS в TACACS + администрирование Отчётов и Действие:



TACACS + конфигурация в WCS

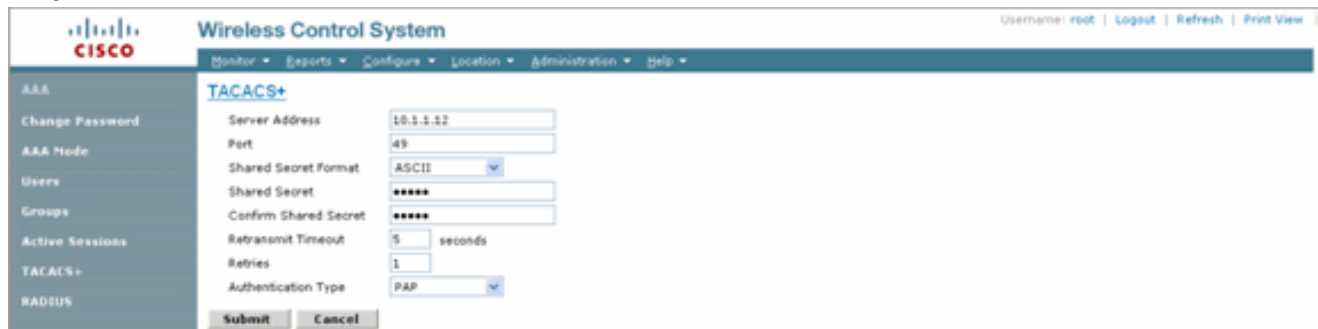
Выполните следующие действия:

1. От GUI войдите к WCS с корневой учетной записью.
2. Добавьте TACACS + сервер. Перейдите к администрированию> AAA>, TACACS + Добавляют TACACS + Сервер.



3. Добавьте TACACS + подробные данные сервера, такие как IP-адрес, номер порта (49

по умолчанию), и общий секретный ключ.



4. Включите TACACS + аутентификация для администрирования в WCS. Перейдите к **администрированию> AAA>, Режим AAA> Выбирает TACACS**

+



[WCS с помощью виртуальных доменов](#)

Виртуальный домен является новой характеристикой, начатой с версии 5.1 WCS. WCS действительный домен состоит из ряда устройств и сопоставляет и ограничивает представление пользователя информацией, относящейся к этим устройствам и картам. Через действительный домен администратор может гарантировать, что пользователи могут только просмотреть устройства и карты, за которые они ответственны. Кроме того, из-за фильтров действительного домена, пользователи могут настроить, обзорные сигналы тревоги, и генерировать отчёты для только своей отведенной роли сети. Администратор задает ряд позволенных действительных доменов для каждого пользователя. Только один из них может быть активным для того пользователя при входе в систему. Пользователь может изменить текущий действительный домен путем выбора другого позволенного действительного домена от раскрывающегося меню виртуального домена наверху экрана. Все отчёты, сигналы тревоги и другая функциональность теперь фильтруются тем действительным доменом.

Если существует только один действительный определенный домен (базируются) в системе, и у пользователя нет действительных доменов в полях настраиваемых атрибутов в TACACS +/RADIUS сервером, пользователю назначают корневой действительный домен по умолчанию.

Если существует несколько действительных доменов, и у пользователя нет указанных атрибутов, то пользователь заблокирован от регистрации. Чтобы позволить пользователю входить, настраиваемые атрибуты виртуального домена должны быть экспортированы в RADIUS/TACACS + сервер.

Окно Virtual Domain Custom Attributes позволяет вам указывать на соответствующие определяемые протоколом данные для каждого действительного домена. Кнопка Export на боковой панели Иерархии виртуального домена предварительно форматирует RADIUS и

TACACS действительного домена + атрибуты. Можно скопировать и вставить эти атрибуты в сервер ACS. Это позволяет, что вы для копирования только применимых действительных доменов к серверу ACS экранируете, и гарантирует, что у пользователей только есть доступ к этим действительным доменам.

Для применения предварительно отформатированного RADIUS, и TACACS + приписывает серверу ACS, выполните шаги, объясненные в [RADIUS виртуального домена и TACACS +](#) раздел [Атрибутов](#).

[Настройте Cisco Secure ACS для Использования WCS](#)

Раздел предоставляет шаги, вовлеченные в TACACS + Сервер ACS, чтобы создать сервисы и настраиваемые атрибуты, и назначить роли на пользователей или группы.

Создание пользователей и группы не объяснено в этом разделе. Предполагается, что пользователи и группы созданы по мере необходимости.

[Конфигурация сети](#)

Выполните следующее действие:

Добавьте IP-адрес WCS как клиента AAA с Механизмом аутентификации как TACACS + (Cisco IOS).

The screenshot shows the Cisco Network Configuration interface. At the top left is the Cisco Systems logo. The main title is "Network Configuration". Below the title is a black bar with the word "Edit". On the left side, there is a vertical menu with various configuration options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled "AAA Client Setup For WCS". It contains several input fields and checkboxes. The "AAA Client IP Address" field is set to "192.168.60.5". The "Key" field is set to "cisco". The "Authenticate Using" dropdown menu is set to "TACACS+ (Cisco IOS)". There are four checkboxes: "Single Connect TACACS+ AAA Client (Record stop in accounting on failure)" is unchecked; "Log Update/Watchdog Packets from this AAA Client" is checked; "Log RADIUS Tunneling Packets from this AAA Client" is checked; and "Replace RADIUS Port info with Username from this AAA Client" is unchecked. At the bottom of the main content area, there are five buttons: "Submit", "Submit + Apply", "Delete", "Delete + Apply", and "Cancel". Below these buttons is a yellow button with a question mark icon and the text "Back to Help".

[Настройка интерфейса](#)

Выполните следующие действия:

1. В меню Interface Configuration выберите TACACS + (Cisco IOS) ссылка.
2. Включите **новые сервисы**.
3. Установите и флажки **Пользователя** и **Флажка Группа**.
4. Введите **беспроводной WCS** для сервиса и **HTTP** для протокола. **Примечание:** HTTP должен быть в КОЛПАЧКАХ.
5. Включите **Advanced TACACS + функции**.



Interface Configuration

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration**
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

- PPP IP
- PPP IPX
- PPP Multilink
- PPP Apple Talk
- PPP VPDN
- PPP LCP
- ARAP
- Shell (exec)
- PIX Shell (pixshell)
- SLIP

New Services

		Service	Protocol
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ciscowlc	common
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Wireless-WCS	HTTP
<input type="checkbox"/>	<input type="checkbox"/>		

Advanced Configuration Options

- Advanced TACACS+ Features

6. Нажмите **Submit** для применения изменений.

User/Group Setup

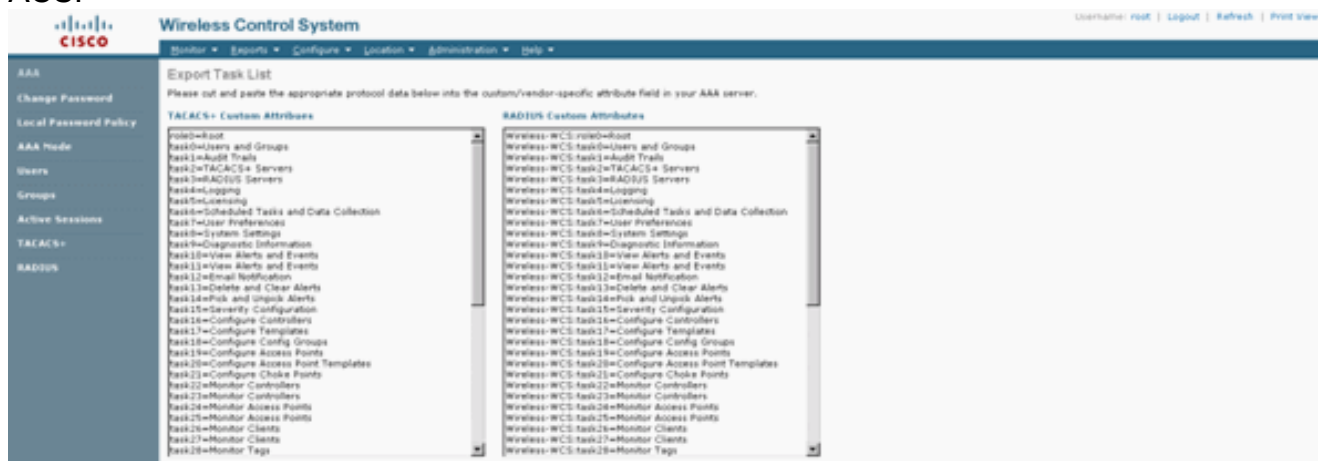
Выполните следующие действия:

1. В GUI WCS перейдите к **администрированию> AAA> Группы** для выбора любой из групп предварительно заданного пользователя, таких как SuperUsers в WCS.

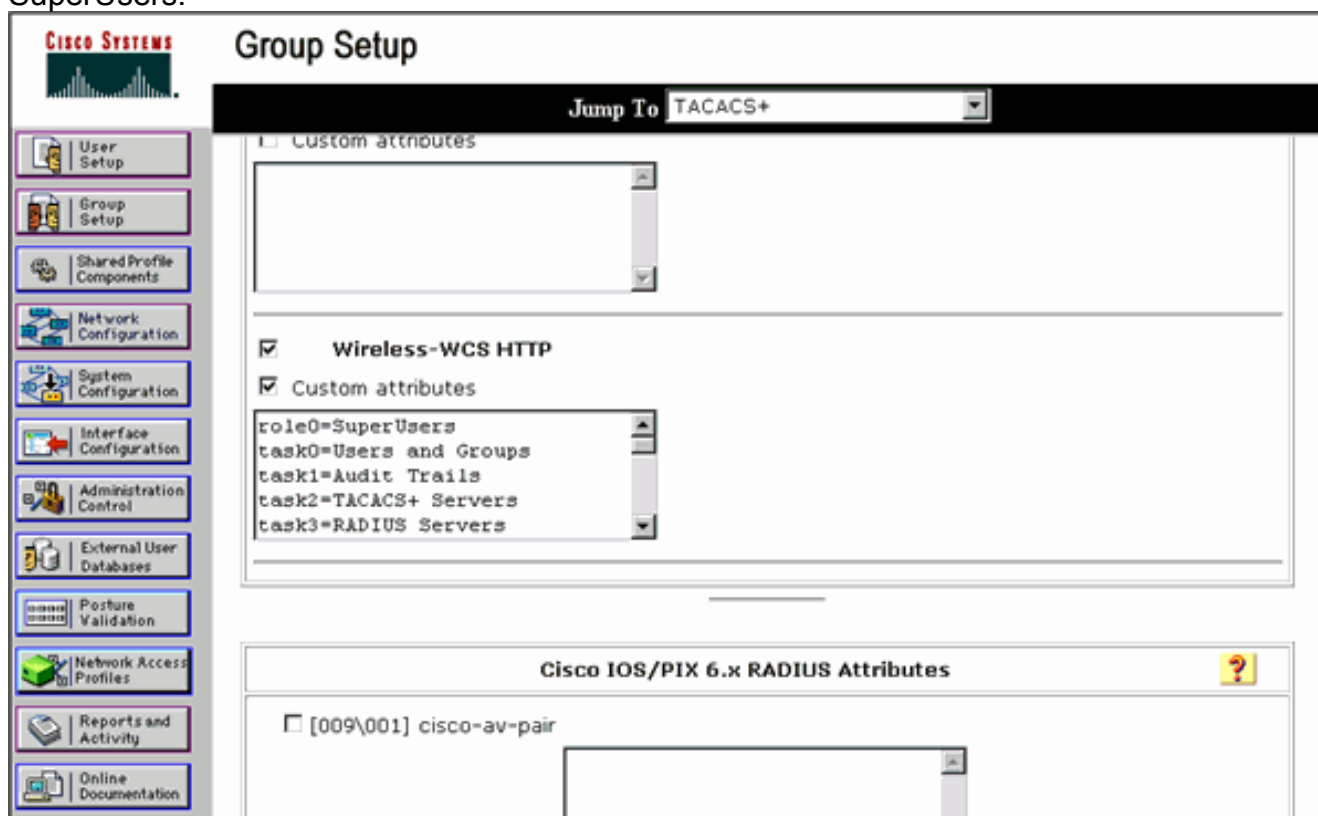
Group Name	Members	Audit Trail	Export
Admin	---		Task List
ConfMasters	---		Task List
Switch_Monitors	---		Task List
Users_Assistant	---		Task List
LethalAmbassador	lbtty ---		Task List
Monitor_Life	---		Task List
North_Sound_AFI	---		Task List
SuperUsers	---		Task List
East	east ---		Task List
User Defined 1	---		Task List
User Defined 2	---		Task List
User Defined 3	---		Task List
User Defined 4	---		Task List

2. Выберите Task List для групп предварительно заданного пользователя и скопируйте

ВСТАВКУ К
ACS.



3. Выберите ранее созданного Пользователя/Группу и перейдите к TACACS + Параметры настройки.
4. В GUI ACS установите флажок, который соответствует сервису беспроводного WCS, который был создан ранее.
5. В GUI ACS установите флажок **Настраиваемых атрибутов**.
6. В текстовом поле ниже Настраиваемых атрибутов введите эту роль и информацию о задаче, скопированную с WCS. Например, введите список задач, разрешенных SuperUsers.



7. Затем войдите к WCS с недавно созданным именем пользователя/паролем в ACS.

[Отладка](#)

[Отладки от WLC для role1=ALL](#)

```
(Cisco Controller) >debug aaa tacacs enable (Cisco Controller) >Wed Feb 28 17:36:37 2007:
```

```
Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:36:37 2007: tplus response: type=1
seq_no=2 session_id=5eaa857e length=16 encrypted=0 Wed Feb 28 17:36:37 2007:
TPLUS_AUTHEN_STATUS_GETPASS Wed Feb 28 17:36:37 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:36:37 2007: processTplusAuthResponse: Continue auth transaction Wed Feb 28
17:36:37 2007: tplus response: type=1 seq_no=4 session_id=5eaa857e length=6 encrypted=0 Wed Feb
28 17:36:37 2007: tplus_make_author_request() from tplus_authen_passed returns rc=0 Wed Feb 28
17:36:37 2007: Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:36:37 2007: author response
body: status=1 arg_cnt=1 msg_len=0 data_len=0 Wed Feb 28 17:36:37 2007: arg[0] = [9][role1=ALL]
Wed Feb 28 17:36:37 2007: User has the following mgmtRole ffffffff8
```

[Отладки от WLC для множественных ролей](#)

```
(Cisco Controller) >debug aaa tacacs enable Wed Feb 28 17:59:33 2007: Forwarding request to
10.1.1.12 port=49 Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=2 session_id=b561ad88
length=16 encrypted=0 Wed Feb 28 17:59:34 2007: TPLUS_AUTHEN_STATUS_GETPASS Wed Feb 28 17:59:34
2007: auth_cont get_pass reply: pkt_length=22 Wed Feb 28 17:59:34 2007:
processTplusAuthResponse: Continue auth transaction Wed Feb 28 17:59:34 2007: tplus response:
type=1 seq_no=4 session_id=b561ad88 length=6 encrypted=0 Wed Feb 28 17:59:34 2007:
tplus_make_author_request() from tplus_authen_passed returns rc=0 Wed Feb 28 17:59:34 2007:
Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:59:34 2007: author response body: status=1
arg_cnt=4 msg_len=0 data_len=0 Wed Feb 28 17:59:34 2007: arg[0] = [11][role1=WLAN] Wed Feb 28
17:59:34 2007: arg[1] = [16][role2=CONTROLLER] Wed Feb 28 17:59:34 2007: arg[2] =
[14][role3=SECURITY] Wed Feb 28 17:59:34 2007: arg[3] = [14][role4=COMMANDS] Wed Feb 28 17:59:34
2007: User has the following mgmtRole 150
```

[Отладки от WLC для сбоя авторизации](#)

```
(Cisco Controller) >debug aaa tacacs enable Wed Feb 28 17:53:04 2007: Forwarding request to
10.1.1.12 port=49 Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=2 session_id=89c553a1
length=16 encrypted=0 Wed Feb 28 17:53:04 2007: TPLUS_AUTHEN_STATUS_GETPASS Wed Feb 28 17:53:04
2007: auth_cont get_pass reply: pkt_length=22 Wed Feb 28 17:53:04 2007:
processTplusAuthResponse: Continue auth transaction Wed Feb 28 17:53:04 2007: tplus response:
type=1 seq_no=4 session_id=89c553a1 length=6 encrypted=0 Wed Feb 28 17:53:04 2007:
tplus_make_author_request() from tplus_authen_passed returns rc=0 Wed Feb 28 17:53:04 2007:
Forwarding request to 10.1.1.12 port=49 Wed Feb 28 17:53:04 2007: author response body:
status=16 arg_cnt=0 msg_len=0 data_len=0 Wed Feb 28 17:53:04 2007: User has the following
mgmtRole 0 Wed Feb 28 17:53:04 2007: Tplus authorization for tac failed status=16
```

[Дополнительные сведения](#)

- [Контроллер беспроводной локальной сети Cisco \(WLC\) и ACS Cisco 5.x \(TACACS +\) пример конфигурации для web-аутентификации](#)
- [TACACS Настройки +](#)
- [Как Настроить Аутентификацию TACACS и Авторизацию для Admin и непользователей Admin в ACS 5.1](#)
- [Сравнение TACACS+ и RADIUS](#)
- [Cisco Systems – техническая поддержка и документация](#)