

# Аутентификация сервера RADIUS пользовательских интерфейсов управления на примере конфигурации контроллера беспроводной локальной сети (WLC)

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Настройка WLC](#)

[Конфигурация Cisco Secure ACS](#)

[Управляйте WLC Локально, а также Через сервер RADIUS](#)

[Проверка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

## Введение

Этот документ поясняет порядок настройки контроллера беспроводных локальных сетей (WLC) и сервера управления доступом (Cisco Secure ACS) для того, чтобы сервер AAA (аутентификации, авторизации и учета) мог выполнять аутентификацию пользователей средств управления на контроллере. Документ также поясняет назначение различных полномочий разным пользователям средств управления с использованием атрибутов поставщика (VSA), возвращаемых сервером RADIUS Cisco Secure ACS.

## 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 как Cisco Secure ACS

## 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

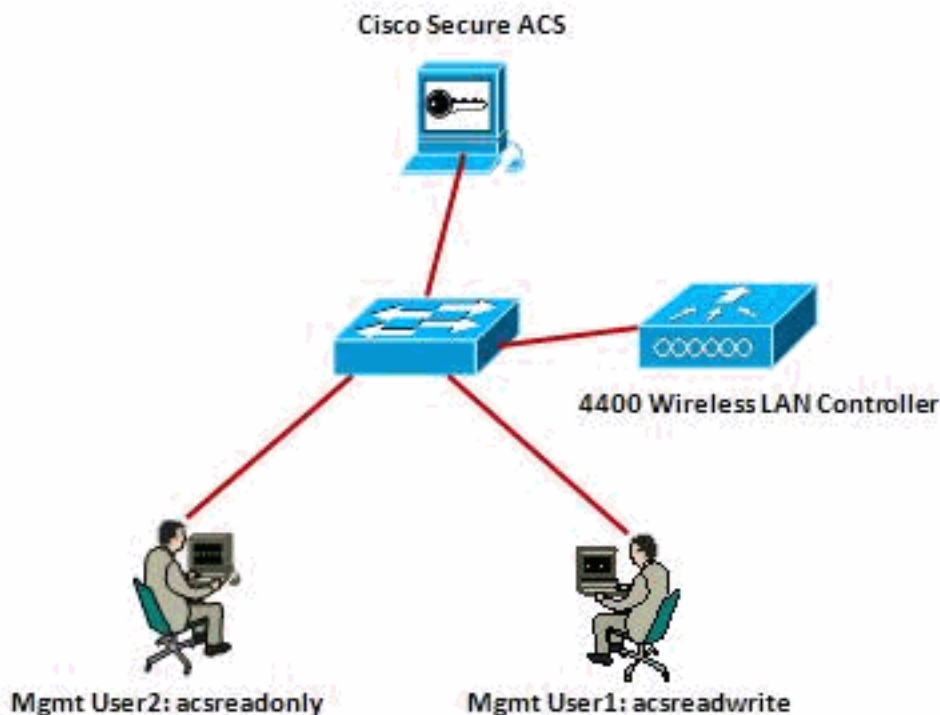
[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

## Настройка

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

## Схема сети

В настоящем документе используется следующая схема сети:



Этот пример конфигурации использует эти параметры:

- IP-адрес Cisco Secure ACS — 172.16.1.1/255.255.0.0
- IP-адрес интерфейса управления контроллера — 172.16.1.30/255.255.0.0
- Общий секретный ключ, который используется на точке доступа (AP) и сервере RADIUS — asdf1234
- Это учетные данные двух пользователей, которых данный пример настраивает на ACS:Имя пользователя - acsreadwriteПароль - acsreadwriteИмя пользователя - acsreadonlyПароль - acsreadonly

Необходимо настроить WLC и Cisco Secure ACS Cisco Secure чтобы к:

- Любому пользователю, который входит в WLC с именем пользователя и паролем как **acsreadwrite**, дают полный административный доступ WLC.
- Любому пользователю, который входит в WLC с именем пользователя и паролем как **acsreadonly**, дают доступ только на чтение WLC.

## [Конфигурации](#)

Эти конфигурации используются в данном документе:

- [Настройка WLC](#)
- [Конфигурация Cisco Secure ACS](#)

## [Настройка WLC](#)

[Настройте WLC для принятия менеджмента через сервер Cisco Secure ACS](#)

Выполните эти шаги для настройки WLC так, чтобы он мог связаться с сервером RADIUS.

1. От GUI WLC нажмите **Security**. Из меню слева, нажмите **RADIUS > Authentication**. Страница **RADIUS Authentication Servers** появляется. Для добавления нового сервера RADIUS нажмите **New**. На странице **RADIUS Authentication Servers > New** введите параметры, определенные для сервера RADIUS. Например.

Security

RADIUS Authentication Servers > New

Server Index (Priority) 1

Server IP Address 172.16.1.1

Shared Secret Format ASCII

Shared Secret

Confirm Shared Secret

Key Wrap  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number 1812

Server Status Enabled

Support for RFC 3576 Enabled

Server Timeout 2 seconds

Network User  Enable

Management  Enable

IPsec  Enable

2. Проверьте кнопку с зависимой фиксацией **Management**, чтобы позволить серверу RADIUS аутентифицировать пользователей, которые входят к WLC. **Примечание:** Гарантируйте, что общий секретный ключ настроил на этой странице соответствия с общим секретным ключом, настроенным на сервере RADIUS. Только тогда WLC может связаться с сервером RADIUS.
3. Проверьте, настроен ли WLC для управления Cisco Secure ACS. Чтобы сделать это, нажмите **Security** от GUI WLC. Результирующее окно GUI кажется подобным данному примеру.

Security

RADIUS Authentication Servers

Call Station ID Type IP Address

Use AES Key Wrap  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter Hyphen

Network User	Management	Server Index	Server Address	Port	IPsec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	172.16.1.1	1812	Disabled	Enabled

1. Call Station ID Type will be applicable only for non 802.1x authentication only.

Вы видите, что флажок **Management** включен для сервера RADIUS 172.16.1.1. Это иллюстрирует, что ACS позволяют аутентифицировать пользовательские интерфейсы управления на WLC.

Выполните шаги в этих разделах для настройки ACS:

1. [Добавьте WLC как клиента AAA к серверу RADIUS.](#)
2. [Настройте пользователей и их соответствующие атрибуты IETF RADIUS.](#)
3. [Настройте пользователя с доступом для чтения-записи.](#)
4. [Настройте пользователя с доступом только на чтение.](#)

### [Добавьте WLC как клиента AAA к серверу RADIUS](#)

Выполните эти шаги для добавления WLC как клиент AAA в Cisco Secure ACS.

1. В графическом интерфейсе ACS выберите Network Configuration (Конфигурация сети).
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. В данном примере это параметры настройки: Имя хоста для клиента AAA является WLC 4400, IP-адрес WLC является 172.16.1.30, который, в этом случае WLC. Общий секретный ключ является "asdf1234".

The screenshot shows the 'Add AAA Client' configuration window in the Cisco Secure ACS Network Configuration interface. The window has a sidebar on the left with various configuration options like 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 area is titled 'Add AAA Client' and contains the following fields and options:

- AAA Client Hostname: WLC-4400
- AAA Client IP Address: 172.16.1.30
- Shared Secret: asdf1234
- RADIUS Key Wrap**
  - Key Encryption Key: [Empty field]
  - Message Authenticator Code Key: [Empty field]
  - Key Input Format:  ASCII  Hexadecimal
- Authenticate Using: RADIUS (Cisco Airespace) [Dropdown menu]
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure):
- Log Update/Watchdog Packets from this AAA Client:
- Log RADIUS Tunneling Packets from this AAA Client:
- Replace RADIUS Port info with Username from this AAA Client:
- Match Framed-IP-Address with user IP address for accounting packets from this AAA Client:

At the bottom of the window, there are three buttons: Submit, Submit + Apply, and Cancel.

Этот общий секретный ключ должен совпасть с общим секретным ключом, который вы настраиваете на WLC.

4. От раскрывающегося меню Используемой аутентификации выберите **RADIUS (Cisco Airespace)**.
5. Нажмите **Submit + Перезапуск** для сохранения конфигурации.

### [Настройте пользователей и их соответствующие атрибуты IETF RADIUS](#)

Для аутентификации пользователя через сервер RADIUS, поскольку контроллер входит и управление, необходимо добавить пользователя к Базе данных RADIUS с набором *Service-Type* атрибута RADIUS IETF к соответствующему значению согласно привилегиям пользователя.

- Для установки привилегий чтения-записи для пользователя установите Атрибут *Service-Type* в **Административный**.
- Для установки привилегий только для чтения для пользователя установите Атрибут *Service-Type* в **Приглашение NAS**.

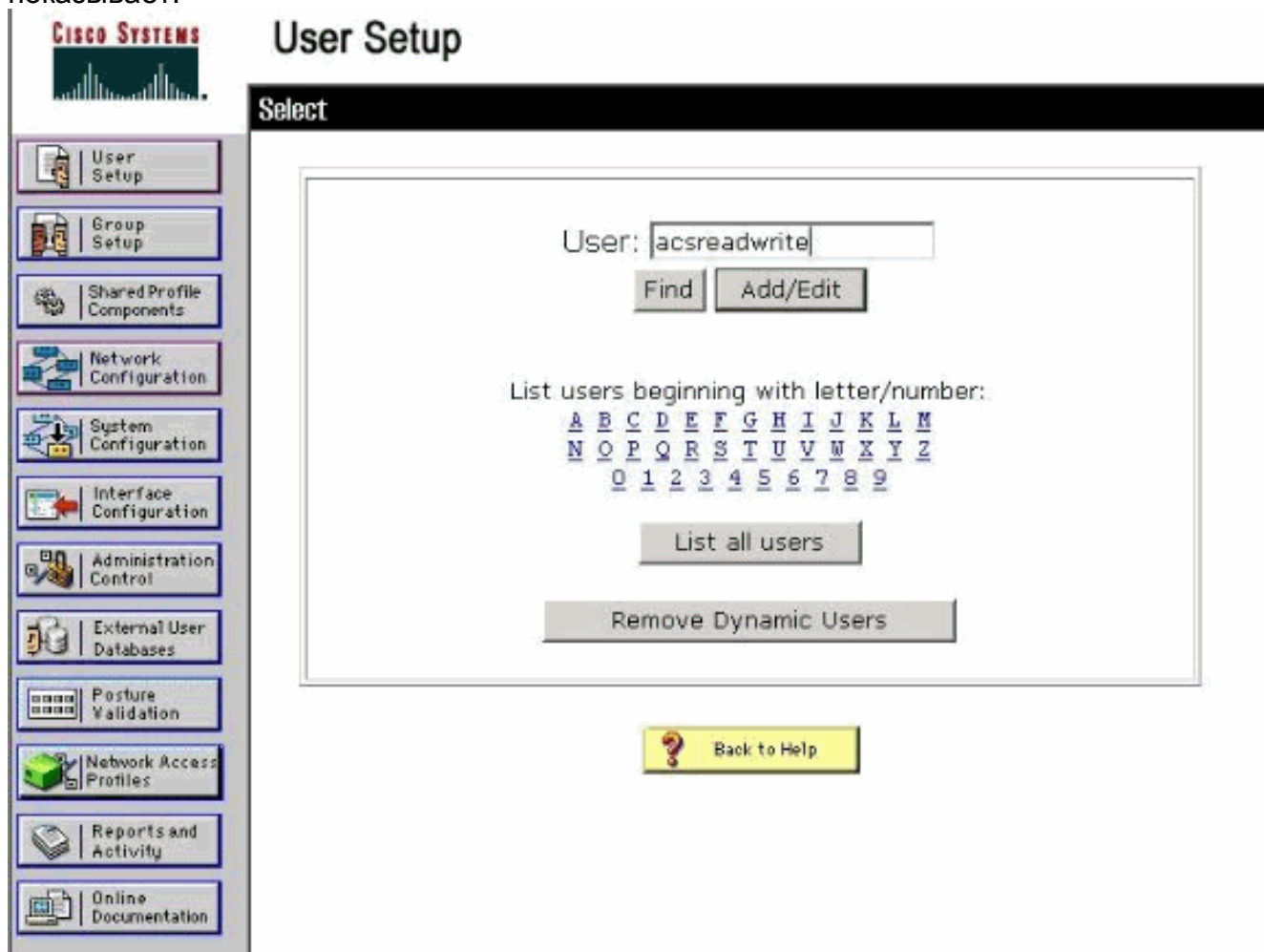
### Настройте пользователя с доступом для чтения-записи

Первый пример показывает конфигурацию пользователя с полным доступом к WLC. Когда этот пользователь пытается войти к контроллеру, сервер RADIUS аутентифицирует и предоставляет этому пользователю полный административный доступ.

В данном примере имя пользователя и пароль является **acsreadwrite**.

Выполните эти шаги на Cisco Secure ACS.

1. В графическом интерфейсе ACS выберите **User Setup (Настройка пользователей)**.
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.
5. Прокрутите вниз к значению Атрибутов RADIUS, стандартизированный IETF и проверьте **Атрибут Service-Type**.
6. С тех пор, в данном примере, пользователь acsreadwrite должен быть предоставленным полным доступом, выбрать **Administrative** для ниспадающего меню Service-Type и нажать **Submit**. Это гарантирует, что у этого индивидуального пользователя есть доступ для чтения-записи к WLC.

Иногда, этот атрибут Service-Type не видим при параметрах пользователя. В таких случаях выполните эти шаги для создания его видимым.

1. От GUI ACS выберите **Interface Configuration > RADIUS (IETF)** для включения атрибутов IETF в окне User Configuration. Это берет вас к RADIUS (IETF) Страница настроек.
2. 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.

**CISCO SYSTEMS**

## Interface Configuration

### RADIUS (IETF)

User	Group
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> [006] Service-Type
<input type="checkbox"/>	<input checked="" type="checkbox"/> [007] Framed-Protocol
<input type="checkbox"/>	<input checked="" type="checkbox"/> [009] Framed-IP-Netmask
<input type="checkbox"/>	<input checked="" type="checkbox"/> [010] Framed-Routing
<input type="checkbox"/>	<input checked="" type="checkbox"/> [011] Filter-Id
<input type="checkbox"/>	<input checked="" type="checkbox"/> [012] Framed-MTU
<input type="checkbox"/>	<input checked="" type="checkbox"/> [013] Framed-Compression
<input type="checkbox"/>	<input checked="" type="checkbox"/> [014] Login-IP-Host
<input type="checkbox"/>	<input checked="" type="checkbox"/> [015] Login-Service
<input type="checkbox"/>	<input checked="" type="checkbox"/> [016] Login-TCP-Port
<input type="checkbox"/>	<input checked="" type="checkbox"/> [018] Reply-Message
<input type="checkbox"/>	<input checked="" type="checkbox"/> [020] Callback-Id
<input type="checkbox"/>	<input checked="" type="checkbox"/> [022] Framed-Route
<input type="checkbox"/>	<input checked="" type="checkbox"/> [023] Framed-IPX-Network
<input type="checkbox"/>	<input checked="" type="checkbox"/> [024] State
<input type="checkbox"/>	<input checked="" type="checkbox"/> [025] Class
<input type="checkbox"/>	<input checked="" type="checkbox"/> [027] Session-Timeout
<input type="checkbox"/>	<input checked="" type="checkbox"/> [028] Idle-Timeout
<input type="checkbox"/>	<input checked="" type="checkbox"/> [029] Termination-Action
<input type="checkbox"/>	<input checked="" type="checkbox"/> [033] Proxy-State
<input type="checkbox"/>	<input checked="" type="checkbox"/> [034] Login-LAT-Service
<input type="checkbox"/>	<input checked="" type="checkbox"/> [035] Login-LAT-Node
<input type="checkbox"/>	<input checked="" type="checkbox"/> [036] Login-LAT-Group

**Примечание:** Данный пример задает аутентификацию на основе для каждого пользователя. Можно также выполнить аутентификацию на основе группы, которой принадлежит индивидуальный пользователь. В таких случаях включите коробку **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](#) для получения дальнейшей информации о том, как настроить и управлять группами.

### [Настройте пользователя с доступом только на чтение](#)

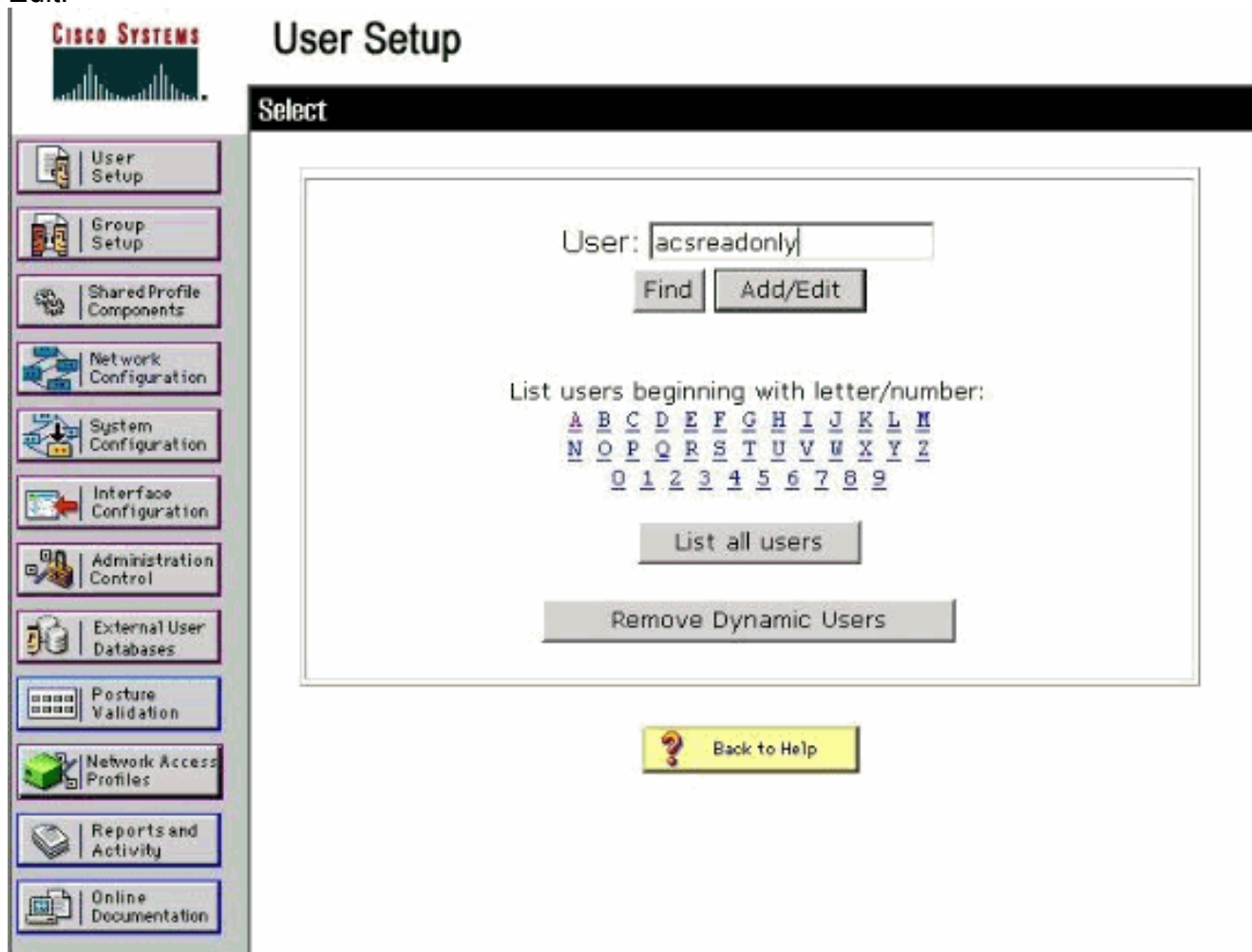
Данный пример показывает конфигурацию пользователя с доступом только на чтение к WLC. Когда этот пользователь пытается войти к контроллеру, сервер RADIUS аутентифицирует и предоставляет этому пользователю доступ только на чтение.



В данном примере имя пользователя и пароль является **acsreadonly**.

Выполните эти шаги на Cisco Secure ACS:

1. В графическом интерфейсе ACS выберите **User Setup (Настройка пользователей)**.
2. Введите имя пользователя, которое вы хотите добавить к ACS и нажать **Add/Edit**, чтобы перейти к Пользовательской странице Edit.



3. Предоставьте Настоящее имя, Описание и Пароль этого пользователя. Это окно показывает пример.

Edit

The screenshot shows the Cisco User Setup interface. On the left is a navigation menu with icons and labels for various configuration areas: 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 'User: acsreadonly (New User)' and contains several sections:

- An 'Account Disabled' checkbox, which is currently unchecked.
- A 'Supplementary User Info' section with a help icon. It contains two text input fields: 'Real Name' with the value 'acsreadonly' and 'Description' with the value 'User with Read only'.
- A 'User Setup' section with a help icon. It includes:
  - A 'Password Authentication:' label.
  - A dropdown menu set to 'ACS Internal Database'.
  - The text: 'CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)'
  - Two password input fields labeled 'Password' and 'Confirm Password', both containing seven dots.
  - An unchecked checkbox labeled 'Separate (CHAP/MS-CHAP/ARAP)'. Below it are two more empty password input fields labeled 'Password' and 'Confirm Password'.
  - A note at the bottom: 'When a token server is used for authentication, supplying a'.

At the bottom of the form are two buttons: 'Submit' and 'Cancel'.

4. Прокрутите вниз к значению Атрибутов RADIUS, стандартизированный IETF и проверьте **Атрибут Service-Type**.
5. С тех пор, в данном примере, пользователь acsreadonly должен иметь доступ только на чтение, выбрать **NAS Prompt** из ниспадающего меню Service-Type и нажать **Submit**. Это гарантирует, что у этого индивидуального пользователя есть доступ только на чтение к WLC.

**CISCO SYSTEMS**

## User Setup

**Account Disable** ?

Never

Disable account if:

Date exceeds: Sep 22 2011

Failed attempts exceed:

Failed attempts since last successful login: 0

Reset current failed attempts count on submit:

---

**IETF RADIUS Attributes** ?

[006] Service-Type

Authenticate only

Authenticate only

NAS Prompt

Outbound

Callback NAS Prompt

Administrative

Callback Administrative

Callback login

Framed

Login

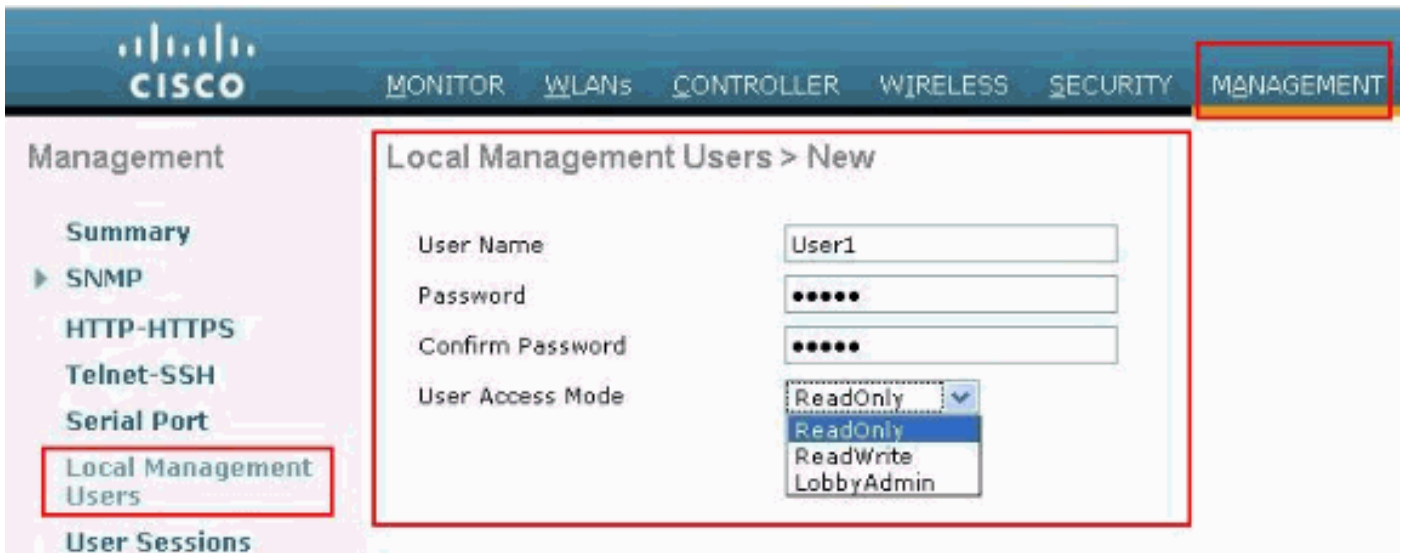
Call Check

Callback framed

Back to Help

### [Управляйте WLC Локально, а также Через сервер RADIUS](#)

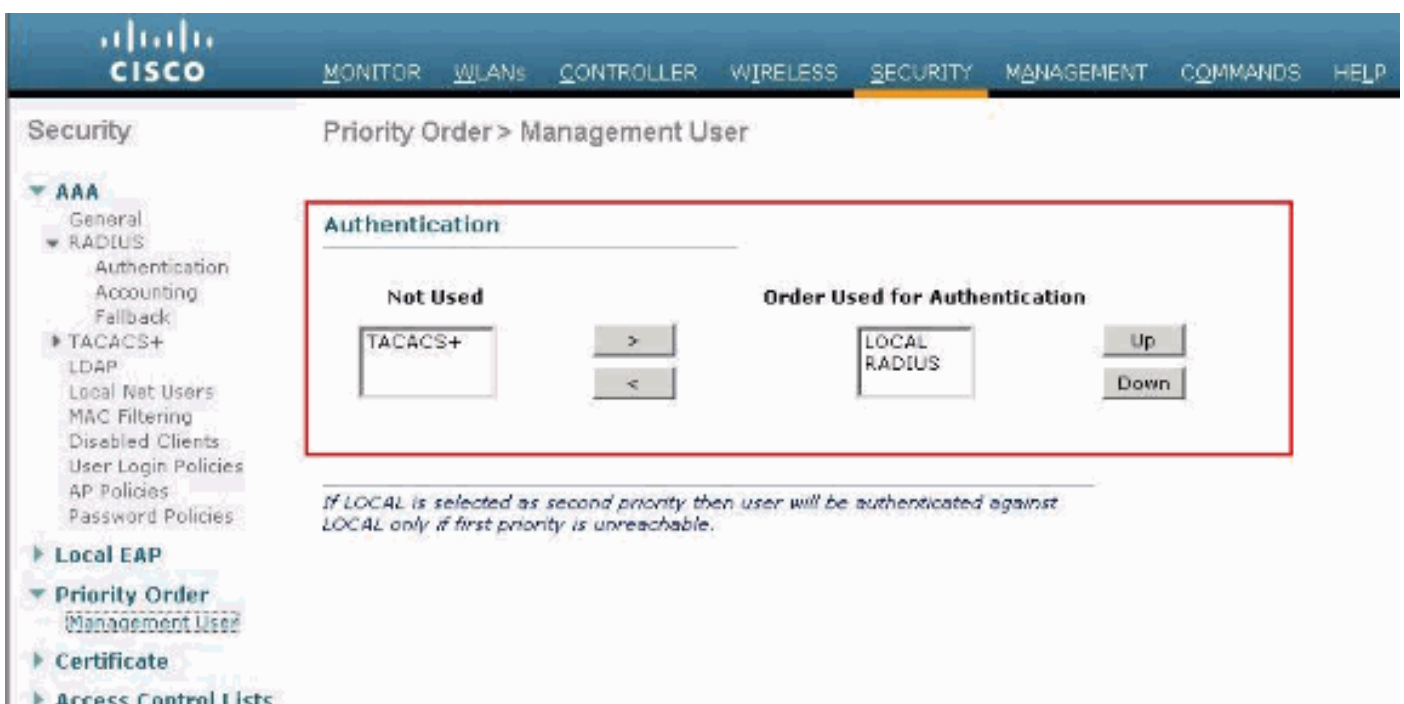
Можно также настроить пользовательские интерфейсы управления локально на WLC. Это может быть сделано от графического интерфейса контроллера под **менеджментом> Пользователи Локального управления**.



Предположите, что WLC настроен с пользовательскими интерфейсами управления оба локально, а также в сервере RADIUS с включенным флажком **Management**. В таком сценарии, по умолчанию, когда пользователь пытается войти к WLC, WLC ведет себя этим способом:

1. WLC сначала посмотрел на пользователей локального управления, определенных для проверки пользователя. Если пользователь существует в его локальном списке, то это позволяет аутентификацию для этого пользователя. Если этот пользователь не появляется локально, то это смотрит на сервер RADIUS.
2. Если тот же пользователь существует оба локально, а также в сервере RADIUS, но с другими привилегиями доступа, то WLC аутентифицирует пользователя с привилегиями, заданными локально. Другими словами, локальная конфигурация на WLC всегда имеет приоритет когда по сравнению с сервером RADIUS.

Заказ аутентификации для пользовательских интерфейсов управления может быть изменен на WLC. Чтобы сделать, это, от страницы **Security** на WLC, нажимает **Priority Order > Management User**. От этой страницы можно задать заказ аутентификации. Например.



**Примечание:** Если **ЛОКАЛЬНЫЙ** выбран как вторая по важности задача, то пользователь

будет аутентифицироваться с помощью этого метода, только если метод, определенный как основная задача (RADIUS / TACACS), недостижим.

## Проверка

Чтобы проверить, работает ли ваша конфигурация должным образом, обратитесь к WLC через CLI или GUI (HTTP/HTTPS) режим. Когда приглашение регистрации появится, введите имя пользователя и пароль согласно конфигурации на Cisco Secure ACS.

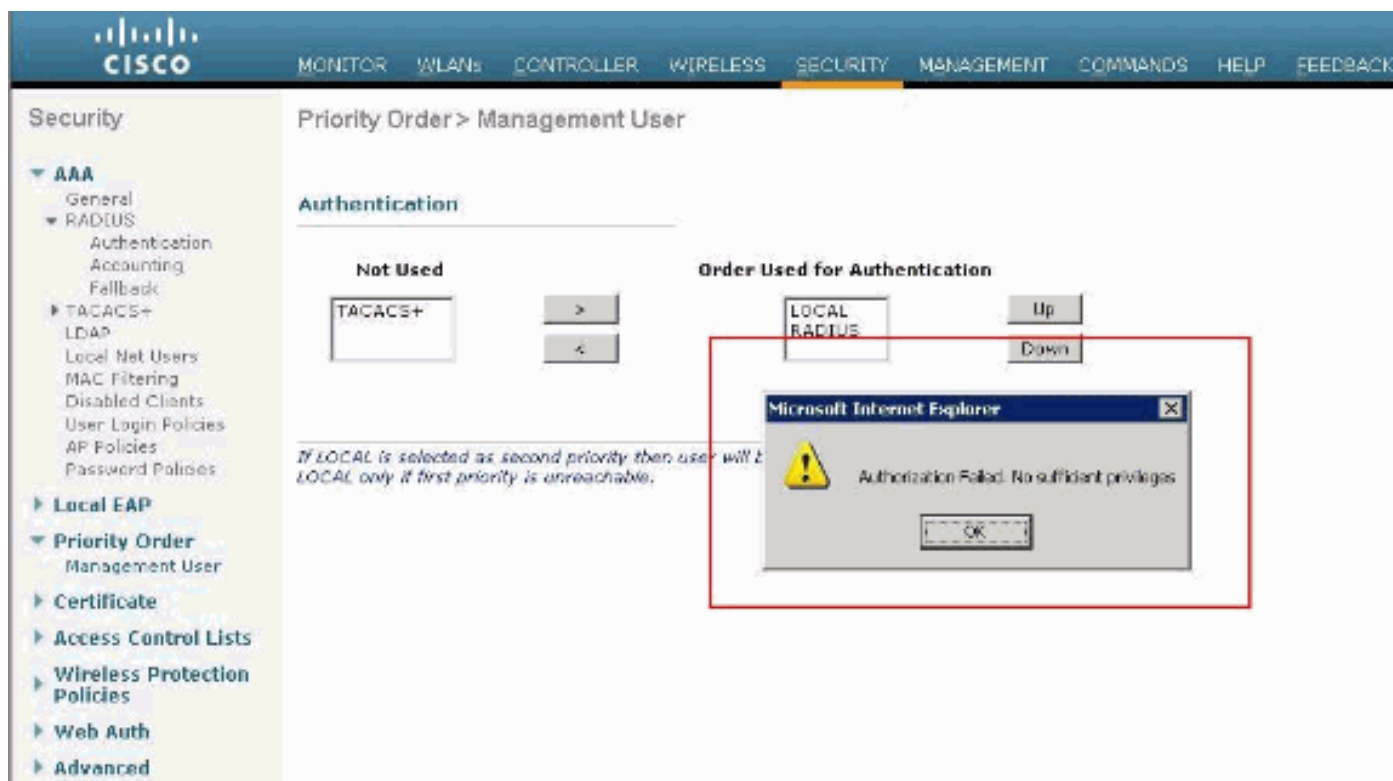
Если у вас есть корректные конфигурации, вы аутентифицируетесь успешно в WLC.

Можно также убедиться, предоставляют ли проверенному пользователю ограничения доступа, как задано ACS. В заказе для этого обращаются, GUI WLC через HTTP/HTTPS (гарантируйте, что WLC настроен для разрешения HTTP/HTTPS).

У пользователя с набором доступа для чтения-записи в ACS есть несколько конфигурируемых привилегий в WLC. Например, у пользователя чтения-записи есть привилегия создать новый WLAN в соответствии со страницей WLANs WLC. Это окно показывает пример.



Когда пользователь с privileges только для чтения пытается изменить конфигурацию на контроллере, пользователь видит это сообщение.



Эти ограничения доступа могут также быть проверены через CLI WLC. Пример представлен в выходных данных.

```
(Cisco Controller) >? debug Manages system debug options. help Help linktest Perform a link test to a specified MAC address. logout Exit this session. Any unsaved changes are lost. show Display switch options and settings. (Cisco Controller) >config Incorrect usage. Use the '?' or <TAB> key to list commands.
```

Поскольку выходные данные данного примера показывают, а? в контроллере CLI отображает список команд, доступных текущему пользователю. Также заметьте, что команда **config** не доступна в выходных данных данного примера. Это иллюстрирует, что у пользователя только для чтения нет привилегии реализовать любые конфигурации на WLC. Принимая во внимание, что, у пользователя чтения-записи действительно есть привилегии реализовать конфигурации на контроллере (и GUI и режим интерфейса командой строки).

**Примечание:** Даже после аутентификации пользователя WLC через сервер RADIUS поскольку вы просматриваете от страницы до страницы, HTTP [S] сервер все еще полностью аутентифицирует клиента каждый раз. Единственная причина вам не предлагают для аутентификации на каждой странице, состоит в том, что ваша кэш-память обозревателя и воспроизводит ваши учетные данные.

## Устранение неполадок

Существуют определенные обстоятельства, когда контроллер аутентифицирует пользовательские интерфейсы управления через ACS, аутентификация заканчивается успешно (**access-accept**), и вы не видите ошибки авторизации на контроллере. *Но, пользователю предлагают снова для аутентификации.*

В таких случаях вы не можете интерпретировать что не так и почему пользователь не может войти в WLC, просто используя команду **debug aaa events enable**. Вместо этого контроллер отображает другое приглашение для аутентификации.

Одна возможная причина для этого - то, что ACS не настроен для передачи атрибута Service-Type для того индивидуального пользователя или группы даже при том, что имя пользователя и пароль правильно настроено на ACS.

Выходные данные команды **debug aaa events enable** не указывают, что у пользователя нет обязательных атрибутов (для данного примера, атрибута Service-Type) даже при том, что **access-accept** передают обратно от AAA-сервера. Выходные данные команды **debug aaa events enable** данного примера показывают пример.

```
(Cisco Controller) >debug aaa events enable Mon Aug 13 20:14:33 2011: AuthenticationRequest: 0xa449a8c Mon Aug 13 20:14:33 2011: Callback.....0x8250c40 Mon Aug 13 20:14:33 2011: protocolType.....0x00020001 Mon Aug 13 20:14:33 2011: proxyState.....1A:00:00:00:00:00-00:00 Mon Aug 13 20:14:33 2011: Packet contains 5 AVPs (not shown) Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Successful transmission of Authentication Packet (id 8) to 172.16.1.1:1812, proxy state 1a:00:00:00:00:00-00:00 Mon Aug 13 20:14:33 2011: ****Enter processIncomingMessages: response code=2 Mon Aug 13 20:14:33 2011: ****Enter processRadiusResponse: response code=2 Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Access-Accept received from RADIUS server 172.16.1.1 for mobile 1a:00:00:00:00:00 receiveId = 0 Mon Aug 13 20:14:33 2011: AuthorizationResponse: 0x9802520 Mon Aug 13 20:14:33 2011: structureSize.....28 Mon Aug 13 20:14:33 2011: resultCode.....0 Mon Aug 13 20:14:33 2011: protocolUsed.....0x00000001 Mon Aug 13 20:14:33 2011: proxyState.....1A:00:00:00:00:00-00:00 Mon Aug 13 20:14:33 2011: Packet
```

contains 0 AVPs:

В этих первых выходных данных команды **debug aaa events enable** в качестве примера вы видите, что Access-Accept успешно получен от сервера RADIUS, но атрибут Service-Type не передают на WLC. Это вызвано тем, что индивидуальный пользователь не настроен с этим атрибутом на ACS.

Cisco Secure ACS должен быть настроен для возврата атрибута Service-Type после проверки подлинности пользователя. Значение атрибута Service-Type должно быть установлено или в **Административный** или в **Быстрый NAS** согласно полномочиям пользователя.

Этот второй пример показывает выходные данные команды **debug aaa events enable** снова. Однако на этот раз атрибут Service-Type установлен в **Административный** на ACS.

```
(Cisco Controller)>debug aaa events enable Mon Aug 13 20:17:02 2011: AuthenticationRequest:
0xa449f1c Mon Aug 13 20:17:02 2011: Callback.....0x8250c40 Mon
Aug 13 20:17:02 2011: protocolType.....0x00020001 Mon Aug 13
20:17:02 2011: proxyState.....1D:00:00:00:00:00-00:00 Mon Aug 13 20:17:02
2011: Packet contains 5 AVPs (not shown) Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Successful
transmission of Authentication Packet (id 11) to 172.16.1.1:1812, proxy state 1d:00:00:00:00:00-
00:00 Mon Aug 13 20:17:02 2011: ****Enter processIncomingMessages: response code=2 Mon Aug 13
20:17:02 2011: ****Enter processRadiusResponse: response code=2 Mon Aug 13 20:17:02 2011:
1d:00:00:00:00:00 Access-Accept received from RADIUS server 172.16.1.1 for mobile
1d:00:00:00:00:00 receiveId = 0 Mon Aug 13 20:17:02 2011: AuthorizationResponse: 0x9802520 Mon
Aug 13 20:17:02 2011: structureSize.....100 Mon Aug 13 20:17:02 2011:
resultCode.....0 Mon Aug 13 20:17:02 2011:
protocolUsed.....0x00000001 Mon Aug 13 20:17:02 2011:
proxyState.....1D:00:00:00:00:00-00:00 Mon Aug 13 20:17:02 2011: Packet
contains 2 AVPs: Mon Aug 13 20:17:02 2011: AVP[01] Service-Type.....0x00000006 (6) (4
bytes) Mon Aug 13 20:17:02 2011: AVP[02] Class..... CISCOACS:000d1b9f/ac100128/acserver (36
bytes)
```

Вы видите в выходных данных данного примера, что атрибут Service-Type передают на WLC.

## [Дополнительные сведения](#)

- [Контроллер беспроводной локальной сети Настройки - руководство по конфигурации](#)
- [Пример конфигурации сетей VLAN на контроллерах беспроводной LAN](#)
- [Пример конфигурации "Dynamic VLAN Assignment with RADIUS Server and Wireless LAN Controller"](#)
- [Пример базовой конфигурации контроллера беспроводной локальной сети и "облегченной" точки доступа](#)
- [Пример настройки виртуальных локальных сетей VLAN AP Group с беспроводными сетевыми картами](#)
- [Cisco Systems – техническая поддержка и документация](#)