Внешняя веб-аутентификация Использование сервера RADIUS

Содержание

Введение

Этот документ объясняет способ выполнения аутентификации на внешней web-странице с использованием внешнего сервера RADIUS.

Предварительные условия

Требования

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

- Базовые знания о конфигурации Облегченных точек доступа (LAP) и WLC Cisco
- Знание того, как установить и настроить внешний веб-сервер
- Знание того, как настроить Cisco Secure ACS

Используемые компоненты

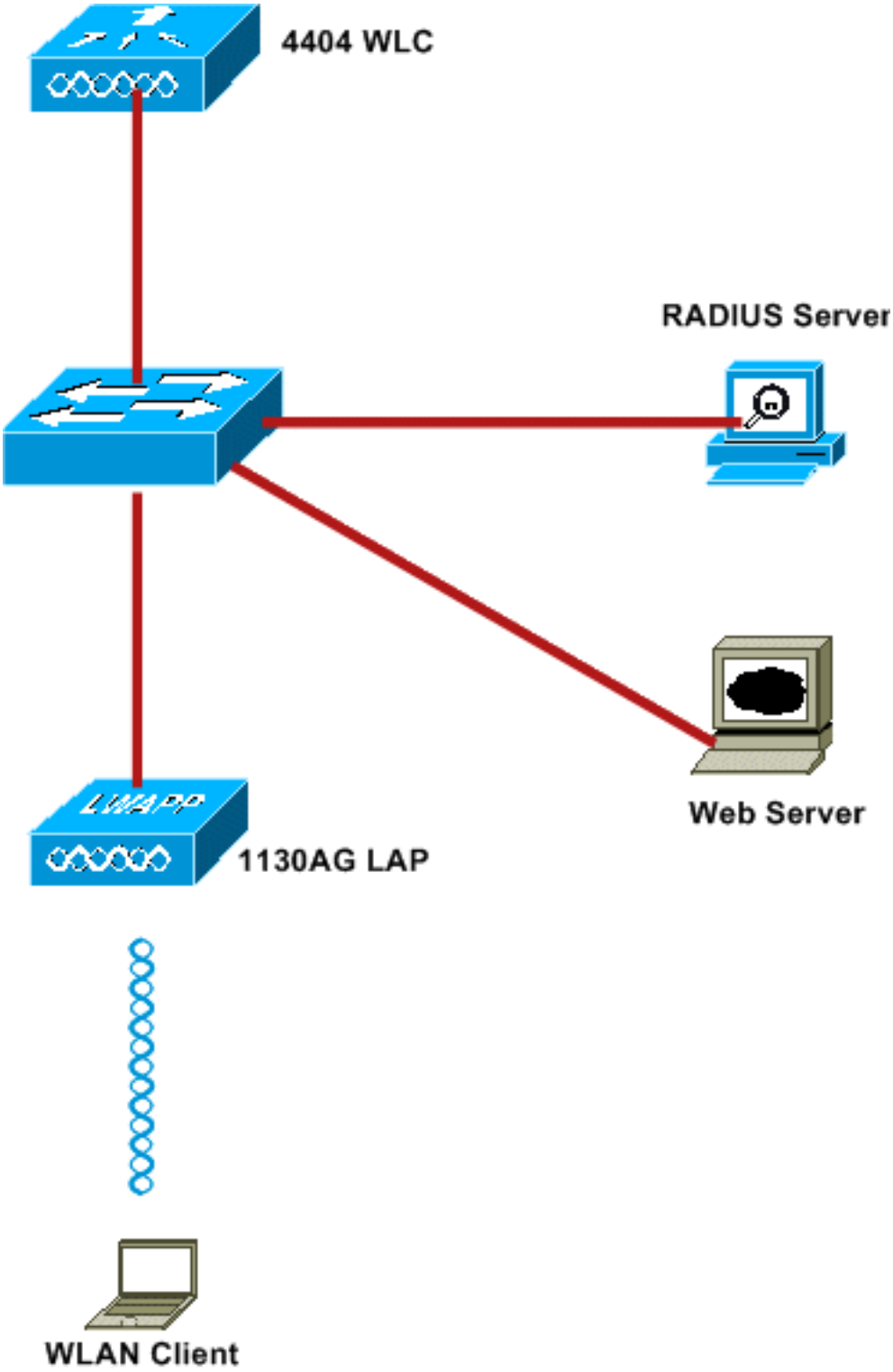
Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Контроллер беспроводной локальной сети, который выполняет Версию микропрограммы 5.0.148.0
- Cisco LAP серии 1232
- Адаптер беспроводного клиента Cisco 802.11a/b/g 3.6.0.61
- Внешний веб-сервер, который размещает страницу для входа в веб-аутентификацию
- Версия Cisco Secure ACS, которая выполняет версию микропрограммы 4.1.1.24

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.

Схема сети

В настоящем документе используется следующая схема сети:



Это IP-адреса, используемые в этом документе:

- WLC использует IP-адрес 10.77.244.206
- LAP зарегистрирован к WLC с IP-адресом 10.77.244.199
- Web-сервер использует IP-адрес 10.77.244.210
- Сервер Cisco ACS использует IP-адрес 10.77.244.196
- Клиент получает IP-адрес от Интерфейса управления, который сопоставлен с WLAN - 10.77.244.208

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Внешняя веб-аутентификация

Web-аутентификация является механизмом аутентификации Уровня 3, используемым для аутентификации гостей для доступа в Интернет. Пользователи аутентифицировались, использование этого процесса не будет в состоянии обратиться к Интернету, пока они успешно не завершат процесс проверки подлинности. Для полной информации на процессе внешней веб-аутентификации считайте Процесс Внешней веб-аутентификации раздела документа Внешняя веб-аутентификация с Примером конфигурации Контроллеров беспроводной локальной сети.

В этом документе мы посмотрели на пример конфигурации, в котором внешняя веб-аутентификация выполнена с помощью внешнего сервера RADIUS.

Настройте WLC

В этом документе мы предполагаем, что WLC уже настроен и зарегистрировал LAP к WLC. Этот документ далее предполагает, что WLC настроен для главной операции и что LAP зарегистрированы к WLC. Если вы - новый пользователь, пытающийся устанавливать WLC для главной операции с LAP, обратитесь к регистрации облегченных точек доступа к Контроллеру беспроводной локальной сети (WLC). Для просмотра LAP, которые зарегистрированы к WLC перейдите к **беспроводным сетям> Все AP**.

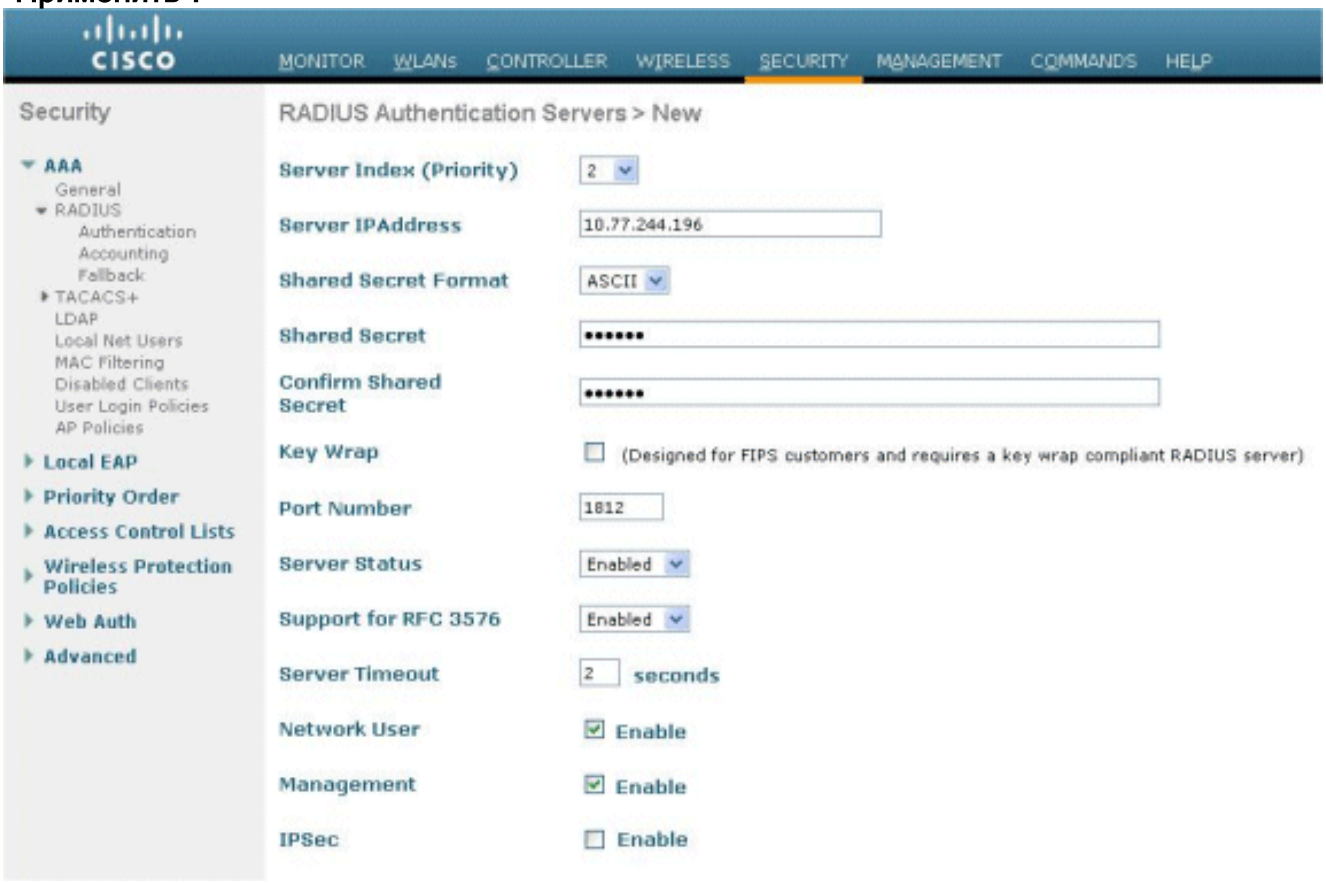
Как только WLC настроен для главной операции и имеет один или несколько LAP, зарегистрированных к ней, можно настроить WLC для внешней веб-аутентификации с помощью внешнего веб-сервера. В нашем примере мы используем версию 4.1.1.24 Cisco Secure ACS в качестве сервера RADIUS. Во-первых, мы настроим WLC для этого сервера RADIUS, и затем мы посмотрим конфигурация, требуемая на Cisco Secure ACS для этой настройки.

Настройте WLC для Cisco Secure ACS

Выполните эти шаги для добавления сервера RADIUS на WLC:

1. От GUI WLC нажмите **МЕНЮ СИСТЕМЫ БЕЗОПАСНОСТИ**.
2. В соответствии с **меню AAA**, перейдите к **Радиусу> Опознавательное** подменю.
3. Нажмите **New** и введите IP-адрес сервера RADIUS. В данном примере IP-адрес сервера *10.77.244.196*.
4. Введите Общий секретный ключ в WLC. Общий секретный ключ должен быть настроен то же на WLC.
5. Выберите **ASCII** или **Hex for Shared Secret Format**. Тот же формат должен быть выбран на WLC.
6. **1812** является Номер порта, используемый для Проверки подлинности RADIUS.
7. Гарантируйте, что опция Server Status установлена во **Включенный**.
8. Проверьте, что Пользователь сети **Позволяет** коробке аутентифицировать пользователей сети.
9. **Щелкните**

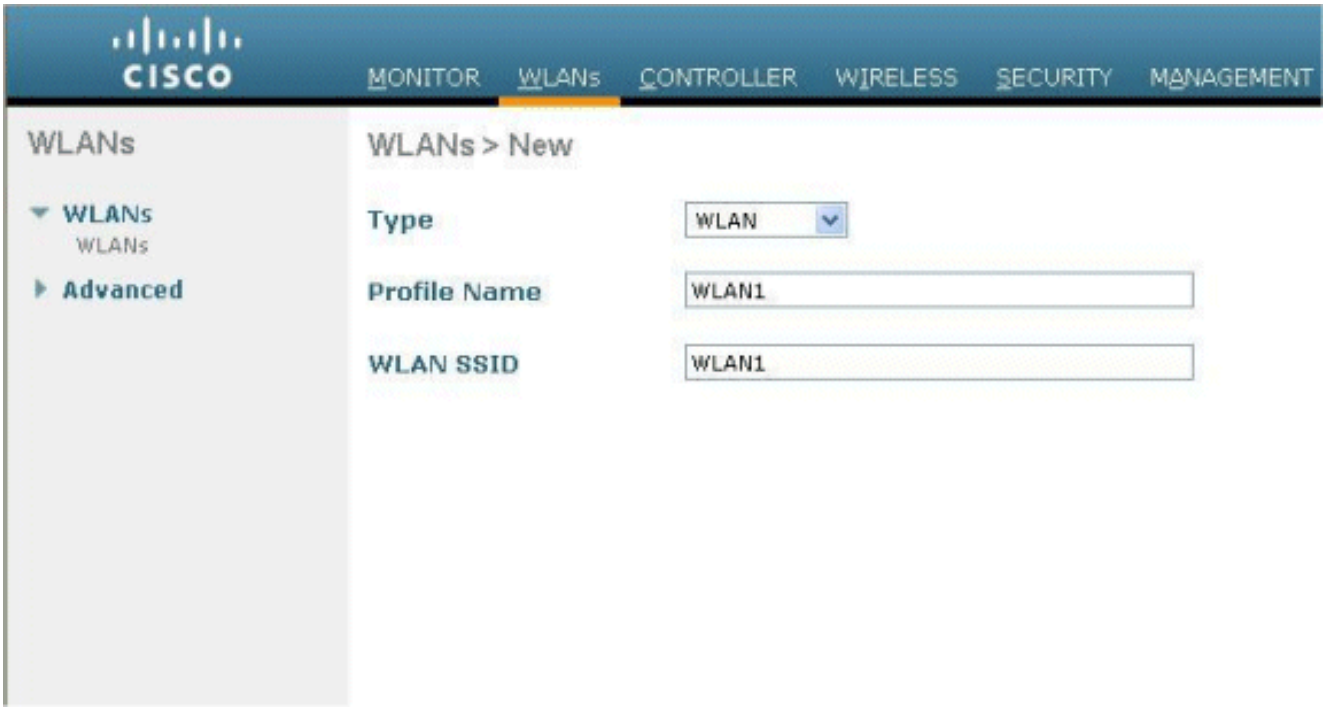
"Применить".



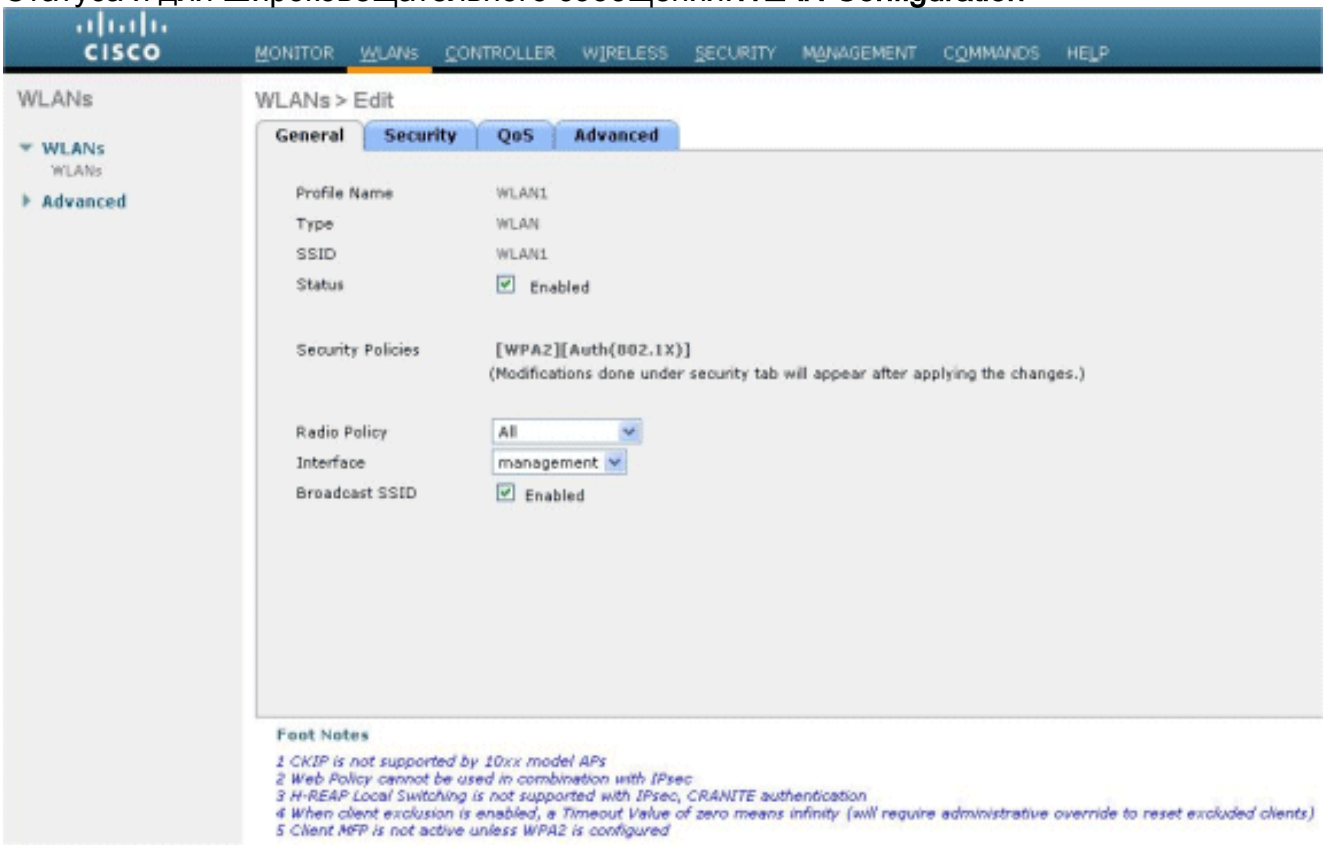
Настройте WLAN на WLC для web-аутентификации

Следующий шаг должен настроить WLAN для web-аутентификации на WLC. Выполните эти шаги для настройки WLAN на WLC:

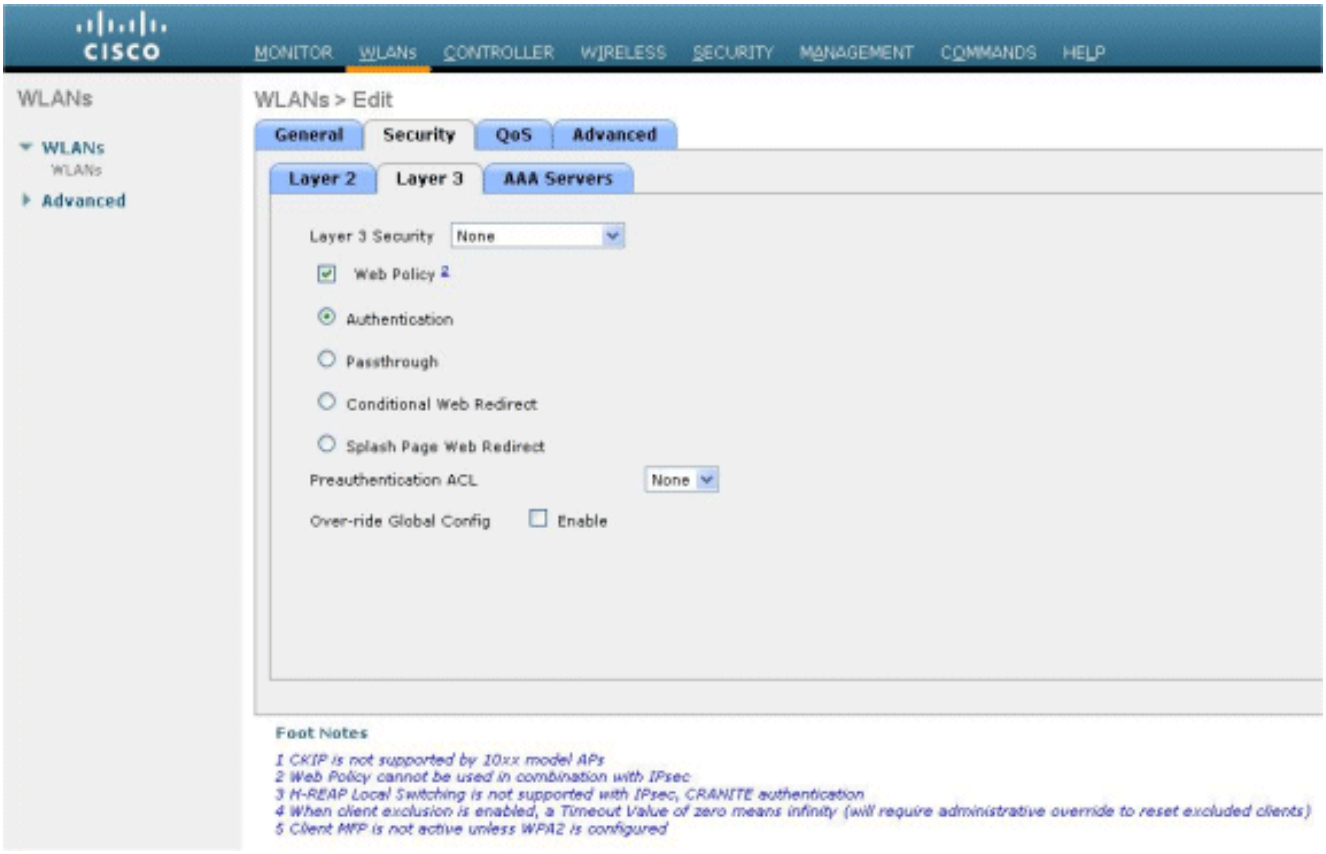
1. Нажмите меню **WLAN** от графического интерфейса контроллера и выберите **New**.
2. Выберите **WLAN for Type**.
3. Введите Имя профиля и SSID WLAN по Вашему выбору, и нажмите **Apply**.**Примечание:** SSID WLAN учитывает регистр.



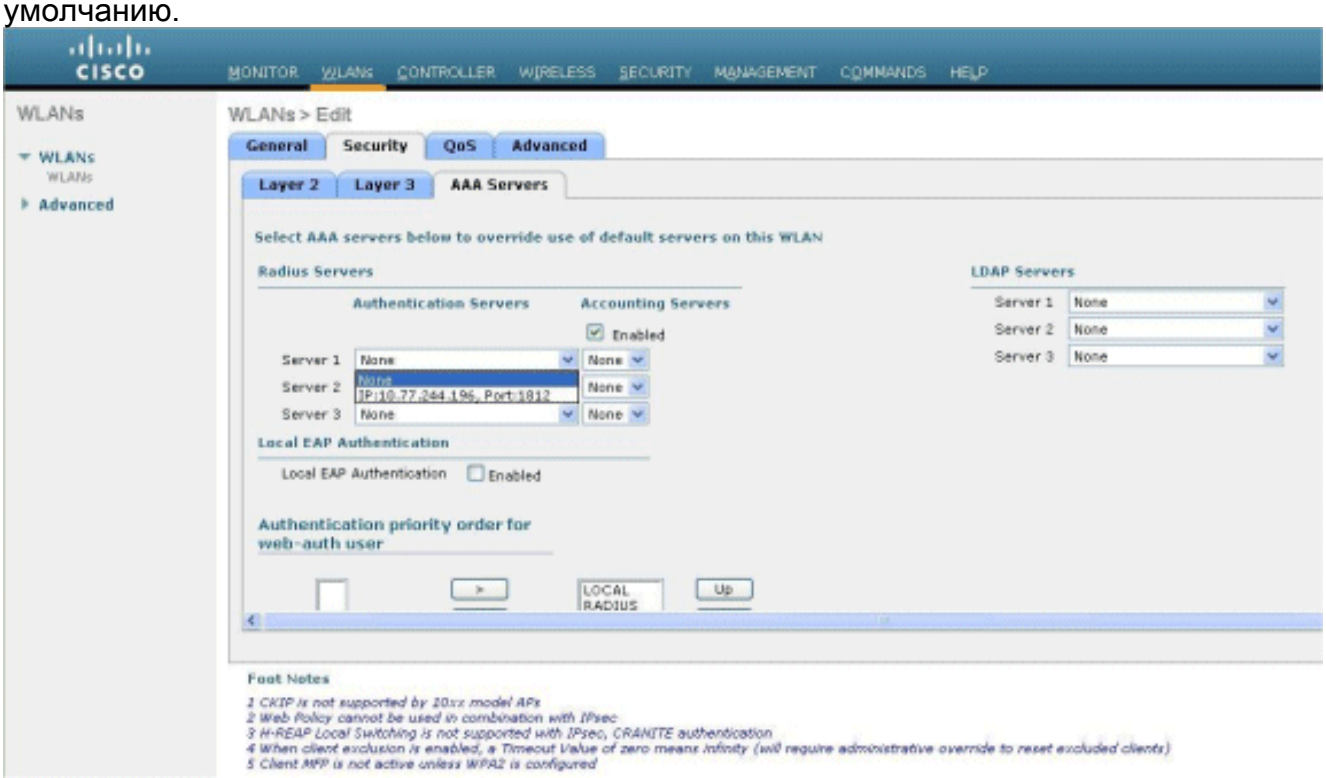
4. Под **Вкладкой Общие** удостоверьтесь, что опция **Enabled** проверена и для SSID Статуса и для Широковещательного сообщения.**WLAN Configuration**



5. Выберите интерфейс для WLAN. Как правило, интерфейс, настроенный в уникальной VLAN, сопоставлен с WLAN так, чтобы клиент получил IP-адрес в той VLAN. В данном примере мы используем *управление* для Интерфейса.
6. Выберите **Вкладку Безопасность**.
7. В соответствии с меню **Уровня 2**, выберите **None for Layer 2 Security**.
8. В соответствии с меню **Уровня 3**, выберите **None for Layer 3 Security**. Проверьте **веб-флажок Policy** и выберите **Authentication**.



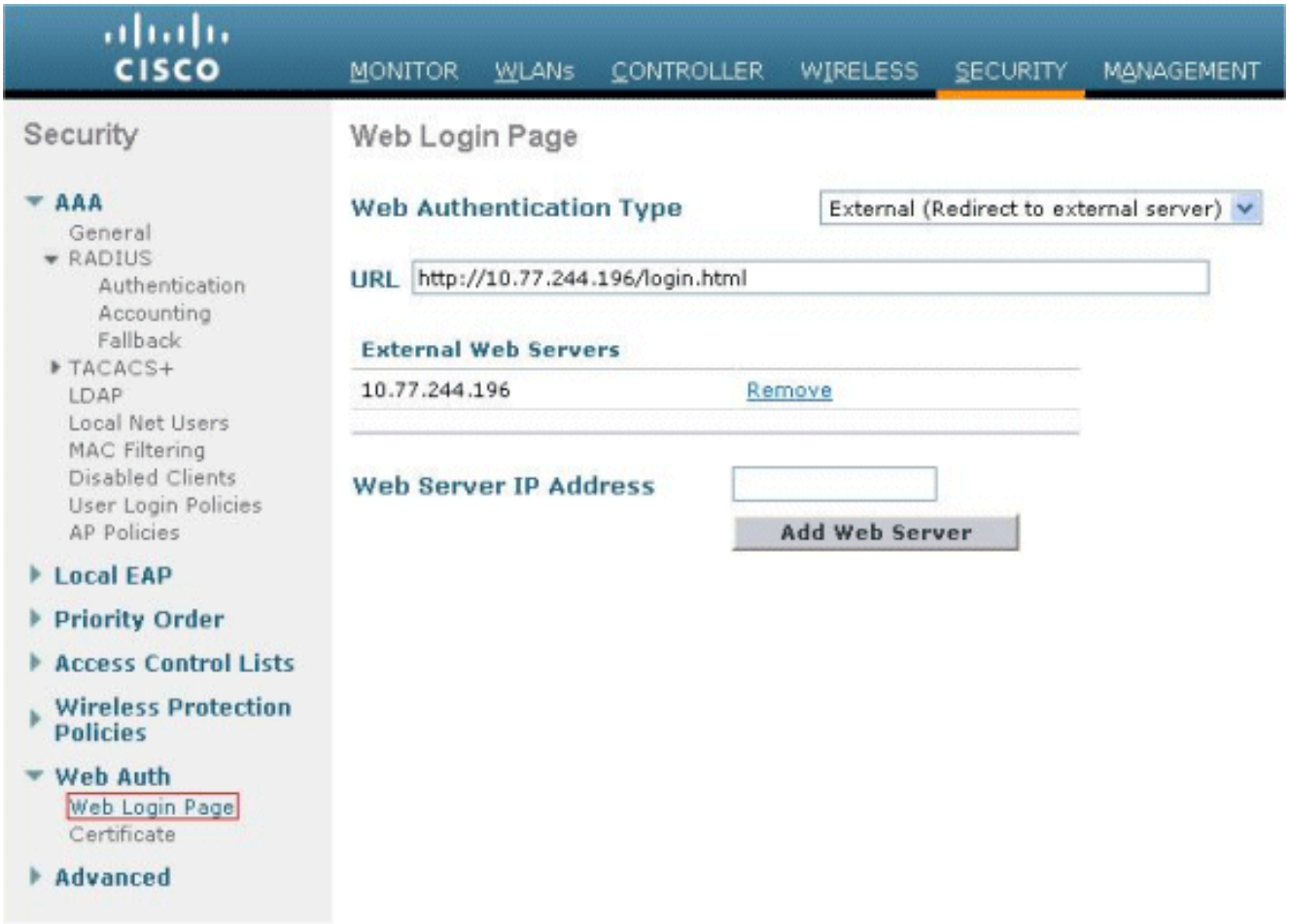
9. В соответствии с меню **AAA-серверов**, для Сервера проверки подлинности, выбирают сервер RADIUS, который был настроен на этом WLC. Другие Меню должны остаться в значениях по умолчанию.



Настройте информацию о Web-сервере о WLC

Web-сервер, который размещает Страницу веб-аутентификации, должен быть настроен на WLC. Выполните эти шаги для настройки Web-сервера:

1. **Щелкните вкладку Безопасность.** Перейдите **к веб-Аутентификации> Веб-страница для входа**.
2. Установите Тип web-аутентификации как **Внешний**.
3. В поле IP Address Web-сервера введите IP-адрес сервера, который размещает Страницу веб-аутентификации, и **нажмите Add Web-сервер**. В данном примере IP-адрес *10.77.244.196*, который появляется под Внешними веб-серверами.
4. Введите URL для Страницы веб-аутентификации (в данном примере, *http://10.77.244.196/login.html*) в поле URL.



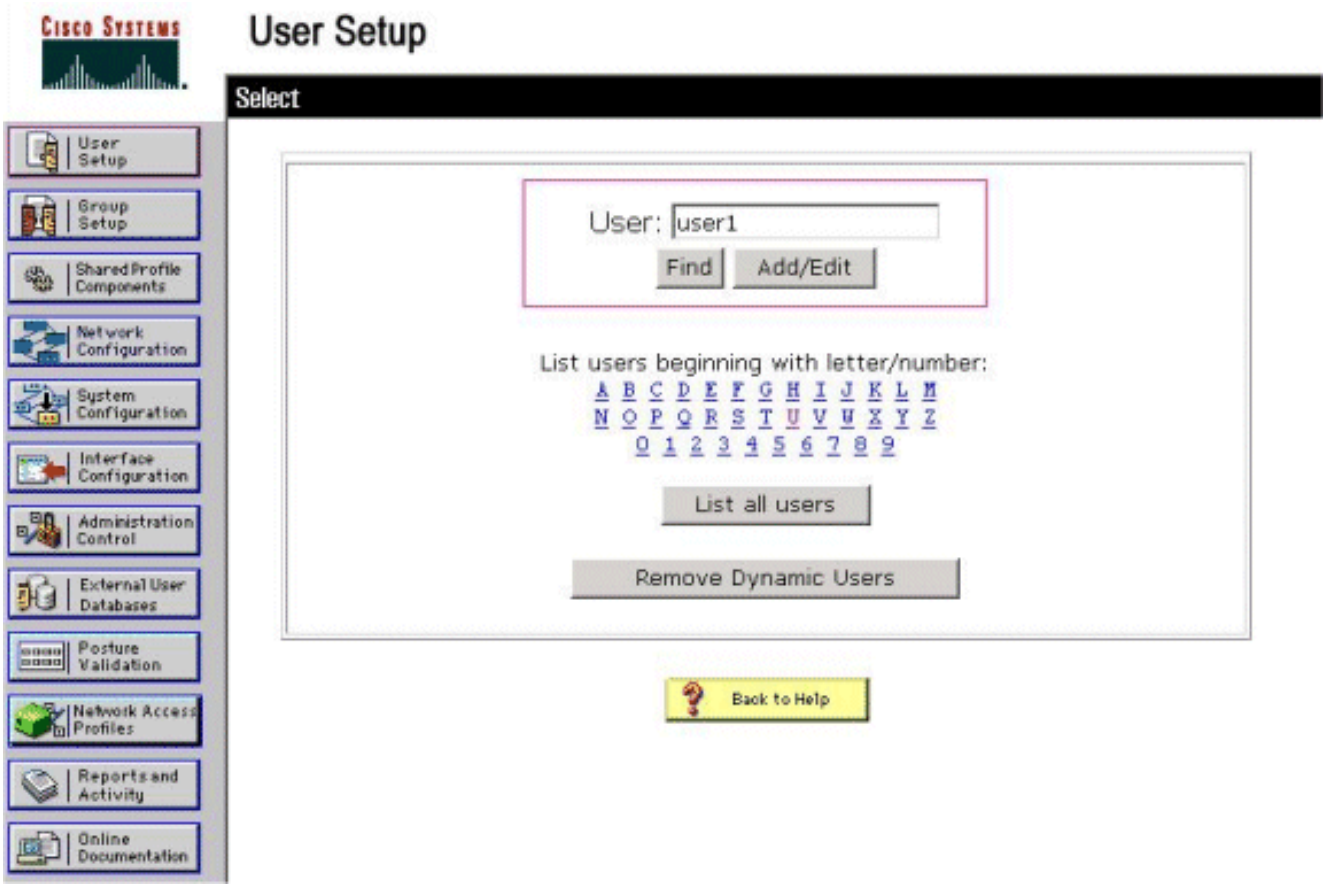
Настройте Cisco Secure ACS

В этом документе мы предполагаем, что Сервер Cisco Secure ACS уже установлен и работа машины. Для получения дополнительной информации, как установить Cisco Secure ACS, обращаются к Руководству по конфигурации для Cisco Secure ACS 4.2.

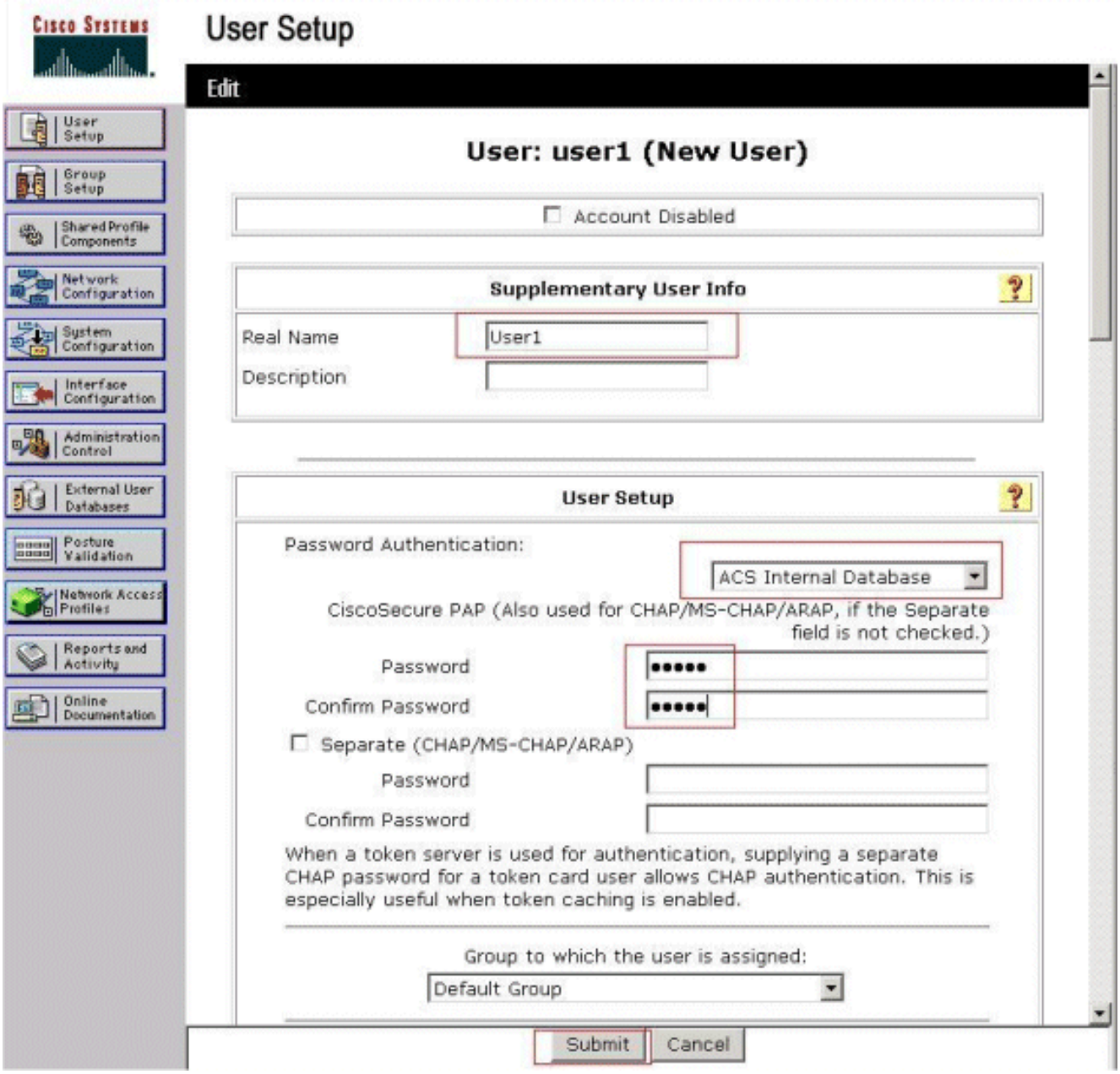
Настройте сведения о пользователе на Cisco Secure ACS

Выполните эти шаги для настройки пользователей на Cisco Secure ACS:

1. Выберите **User Setup** из GUI Cisco Secure ACS, введите имя пользователя и нажмите **Add/Edit**. В данном примере пользователь является *user1*.



2. По умолчанию PAP используется для аутентификации клиентов. Пароль для пользователя введен при **Настройке пользователя> Проверка подлинности с помощью пароля> PAP Cisco Secure**. Удостоверьтесь, что вы выбираете **ACS Internal Database for Password Authentication**.



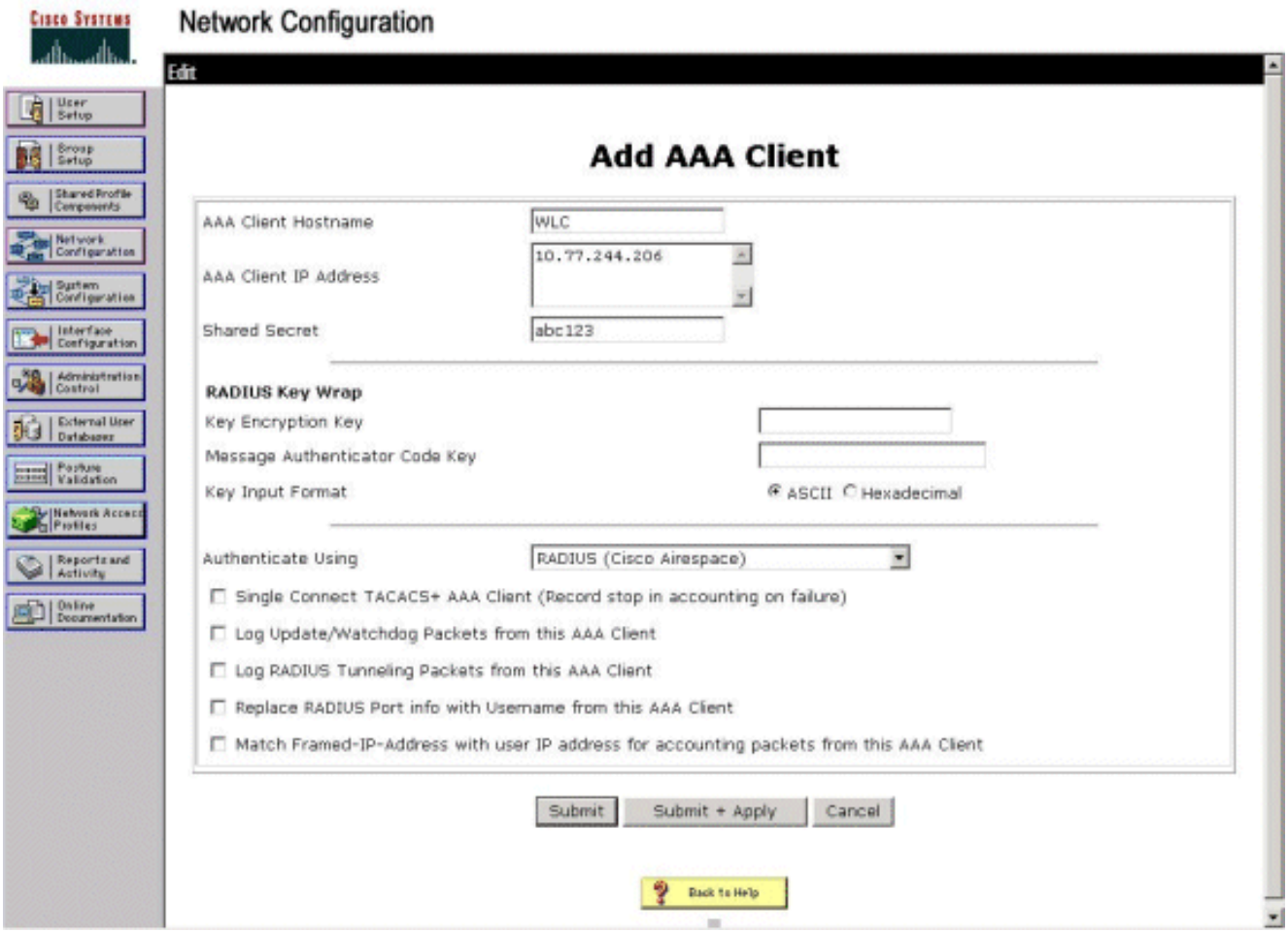
3. Пользователю нужно назначить группа, которой принадлежит пользователь. Выберите **Группу по умолчанию**.
4. **Нажмите кнопку Submit (Отправить).**

Настройте информацию о WLC о Cisco Secure ACS

Выполните эти шаги для настройки информации о WLC о Cisco Secure ACS:

1. В GUI ACS нажмите вкладку **Network Configuration** и **нажмите Add Запись**.
2. Добавить экран клиента AAA появляется.
3. Введите имя клиента. В данном примере мы используем *WLC*.
4. Введите IP-адрес клиента. IP-адрес WLC *10.77.244.206*.
5. Введите Общий секретный ключ и формат ключа. Это должно совпасть с записью, сделанной в **Меню системы безопасности** WLC.
6. Выберите **ASCII** для Ключевого Формата ввода, который должен быть тем же на WLC.
7. Выберите **RADIUS (Cisco Airespace)** для Используемой аутентификации для установки протокола, используемого между WLC и сервером RADIUS.
8. **Нажмите кнопку Submit+Apply (Отправить и**

применить).

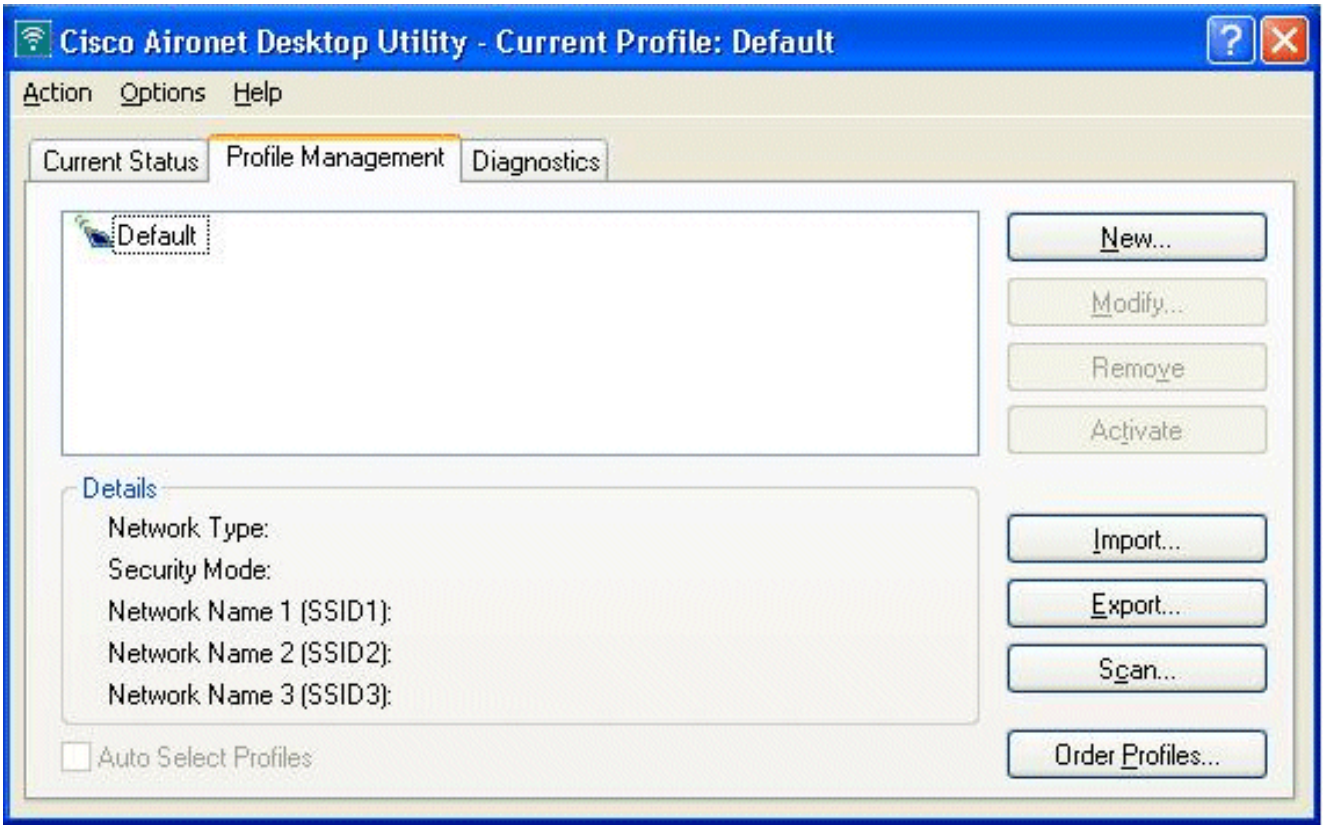


Процесс аутентификации клиента

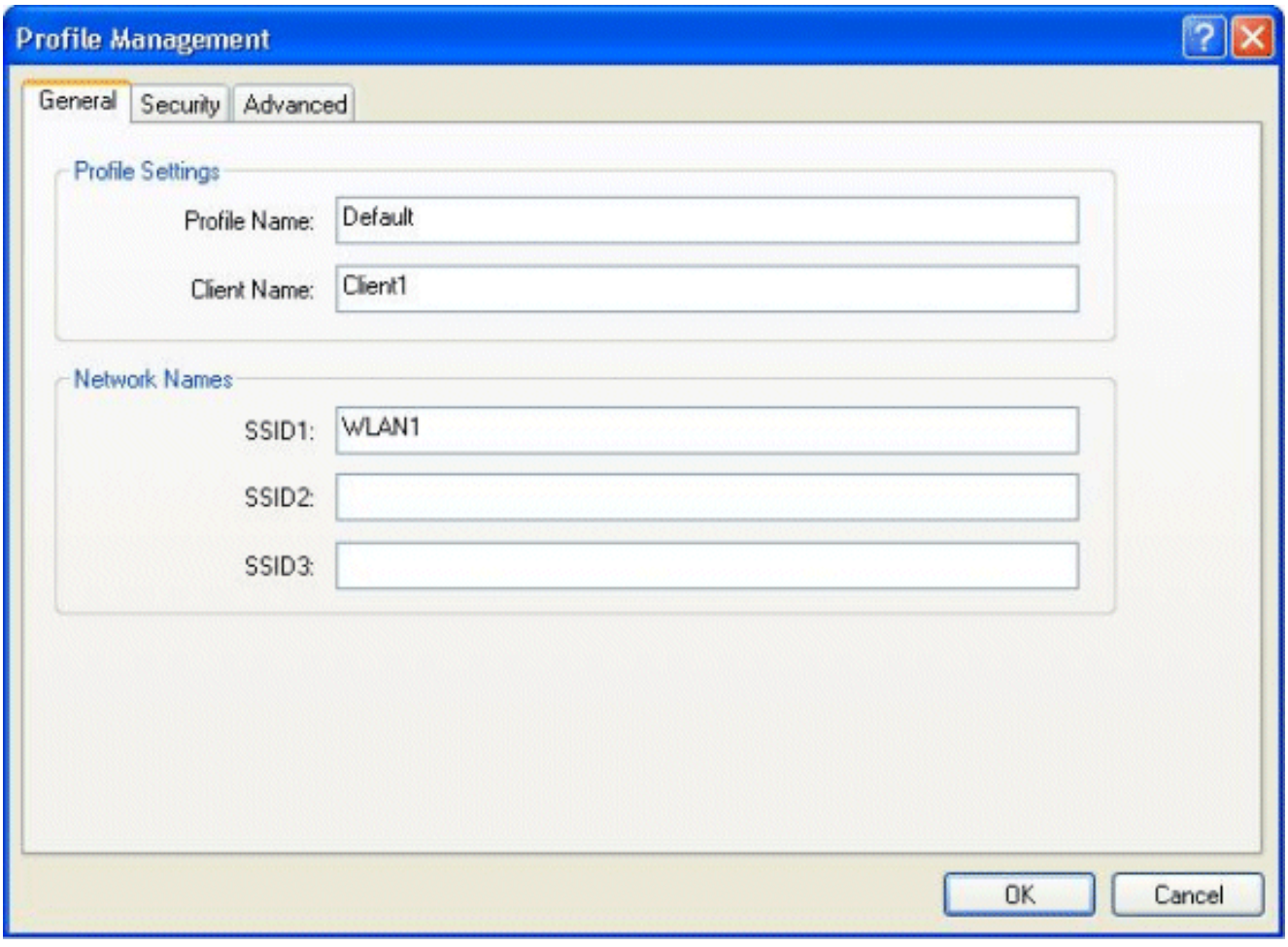
Конфигурация клиента

В данном примере мы используем утилиту Cisco Aironet Desktop Utility для выполнения web-аутентификации. Выполните эти шаги для настройки служебной программы рабочего стола Aironet.

1. Откройте служебную программу рабочего стола Aironet от **Запуска> Cisco Aironet> служебная программа рабочего стола Aironet**.
2. Щелкните по вкладке **Profile Management**.

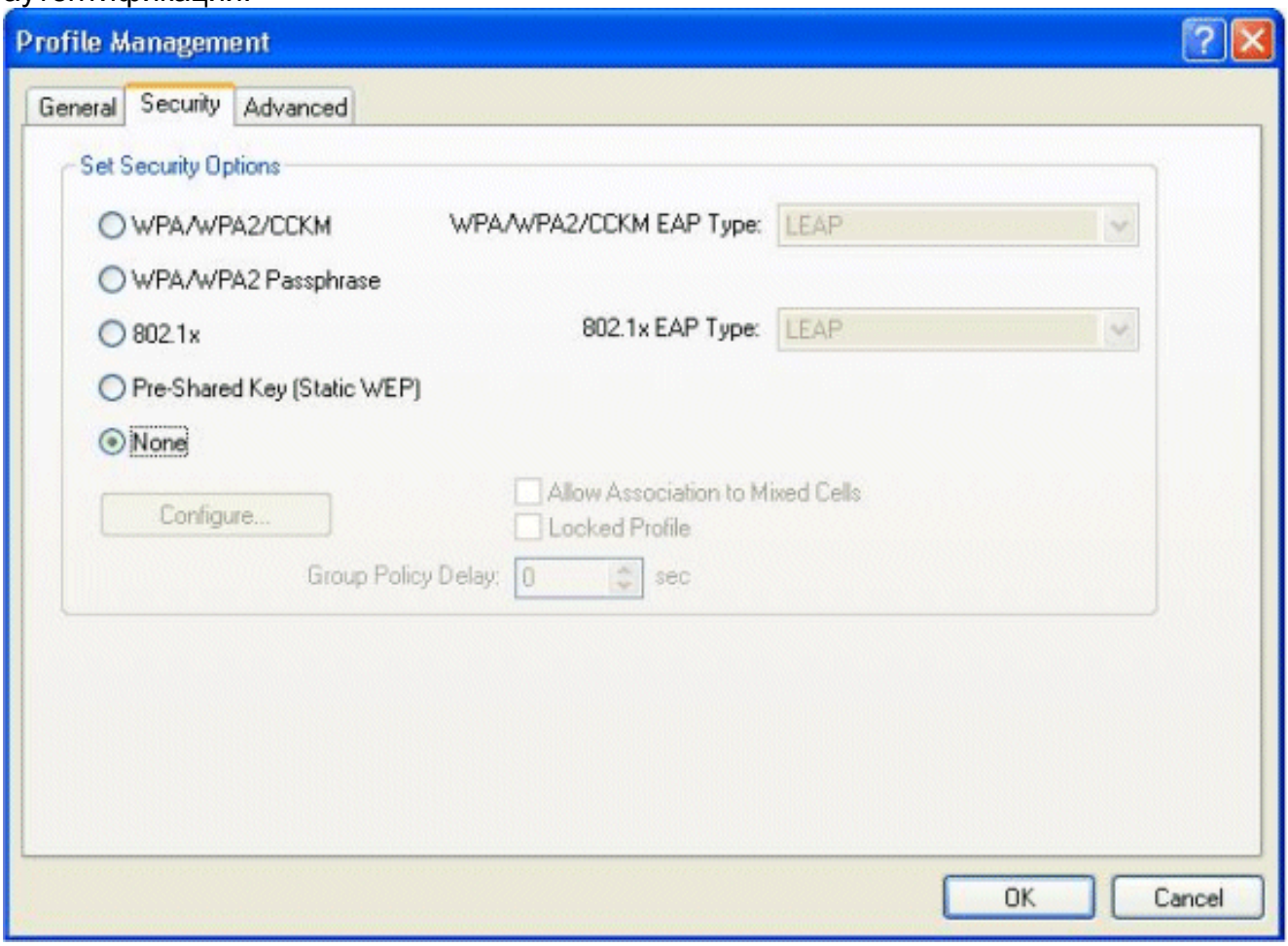


3. Выберите **Профиль по умолчанию** и нажмите **Modify**.Нажмите **Вкладку Общие**.Настройте Имя профиля. В данном примере используется *По умолчанию*.Настройте SSID под Сетевыми именами. В данном примере используется *WLAN1*.

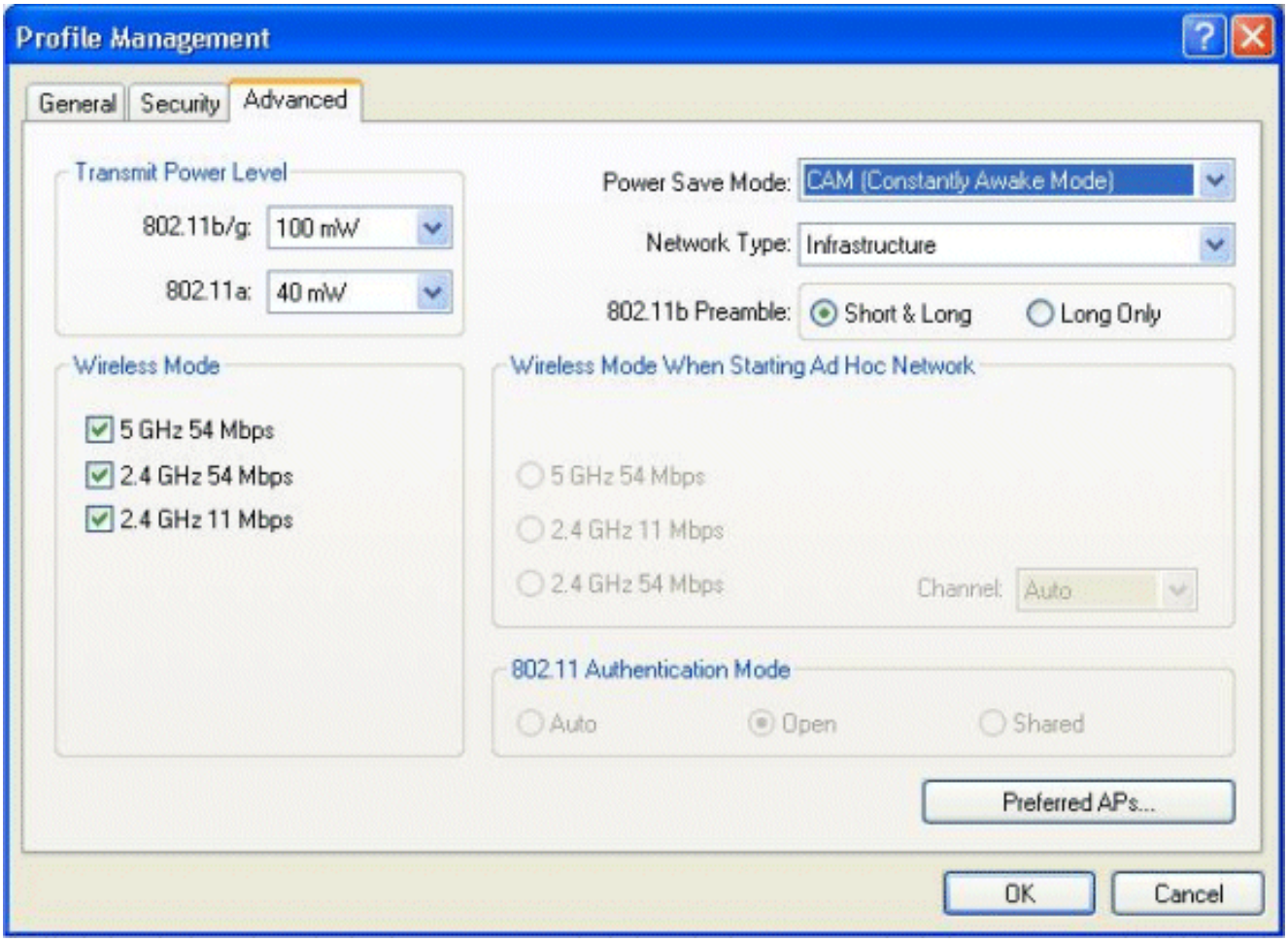


Примечание: SSID учитывает регистр, и он должен совпасть с WLAN, настроенным на WLC.**Щелкните вкладку Безопасность.**Выберите **None** в качестве Безопасности для

web-
аутентификации.



Щелкните вкладку Advanced ("Дополнительно").В соответствии с меню **Wireless Mode**, выберите частоту, в которой беспроводной клиент связывается с LAP.Под **Уровнем мощности передачи** выберите Power, который настроен на WLC.Оставьте значение по умолчанию для Питания, Сохраняют Режим.Выберите **Infrastructure** в качестве типа сети.Установите 802.11b Преамбула как **Short & Long for** лучшая совместимость.**Нажмите кнопку**
ОК.

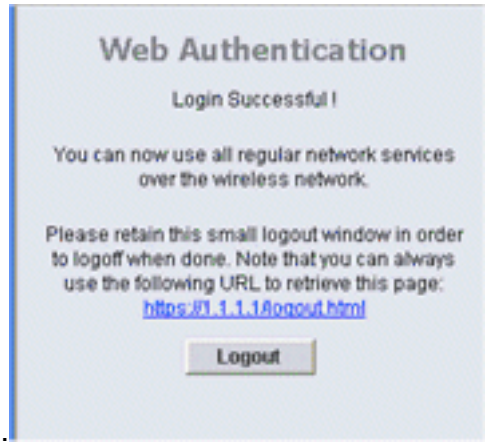


4. Как только Профиль настроен на клиентском программном обеспечении, клиент привязан успешно и получает IP-адрес от пула VLAN, настроенного для интерфейса управления.

Процесс входа в систему клиента

Этот раздел объясняет, как происходит вход в систему клиента.

1. Откройте окно браузера и введите любой URL или IP-адрес. Это приносит страницу веб-аутентификации клиенту. Если контроллер выполняет какой-либо выпуск ранее, чем 3.0, пользователь должен ввести *https://1.1.1.1/login.html* для внедрения страницы веб-аутентификации. Окно сигнала о нарушении безопасности отображается.
2. **Для продолжения нажмите кнопку Yes (Да).**
3. Когда окно Login появляется, введите имя пользователя и пароль, которое настроено на сервере RADIUS. Если ваш вход в систему будет успешен, то вы будете видеть два окна браузера. Большее окно указывает на успешную регистрацию в системе, и вы можете это окно для просмотра Интернета. Используйте меньшее окно, чтобы выйти из системы, когда ваше использование гостевой сети

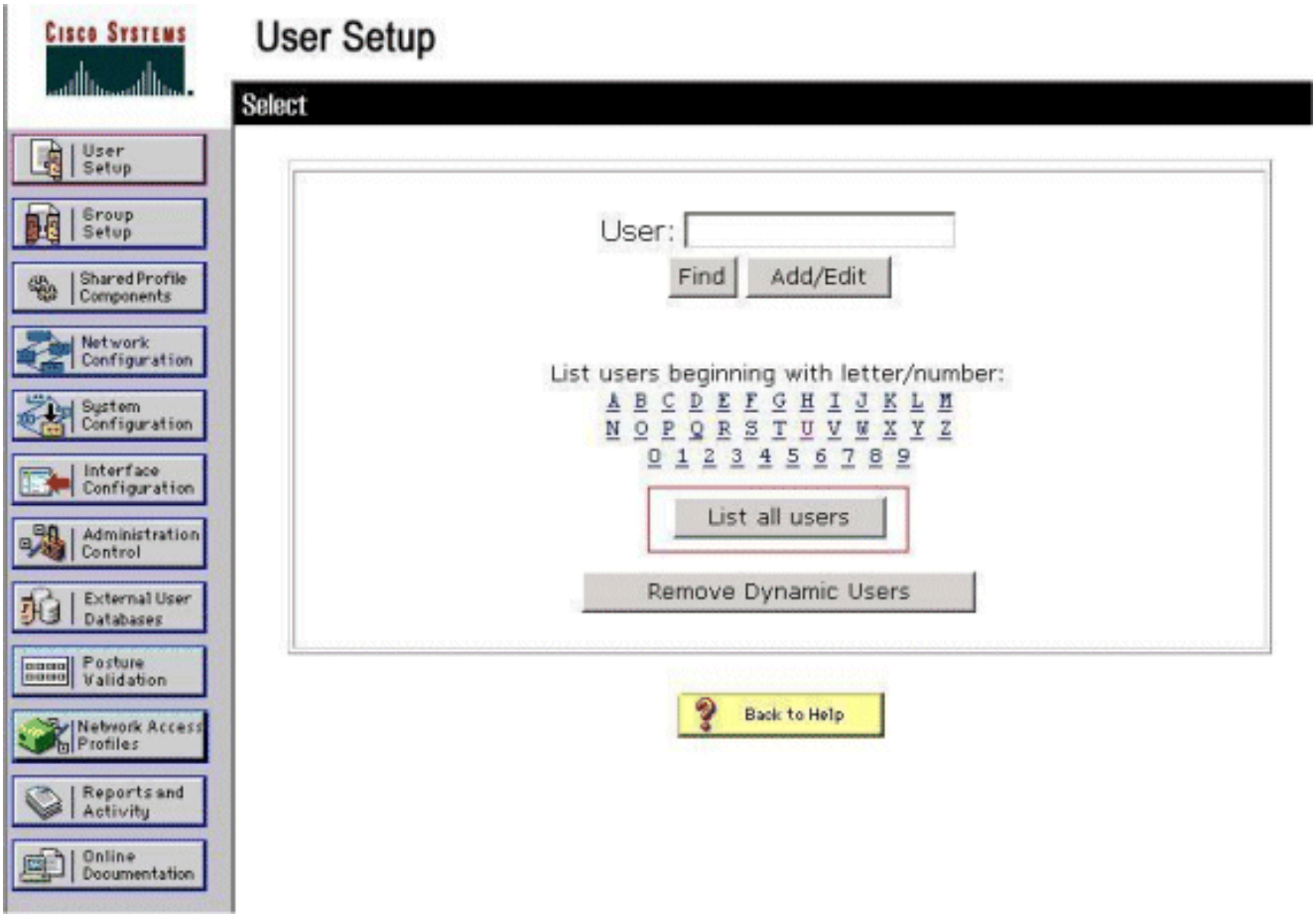
завершено. 

Проверка

Для успешной web-аутентификации необходимо проверить, настроены ли устройства соответствующим способом. Этот раздел объясняет, как проверить устройства, используемые в процессе.

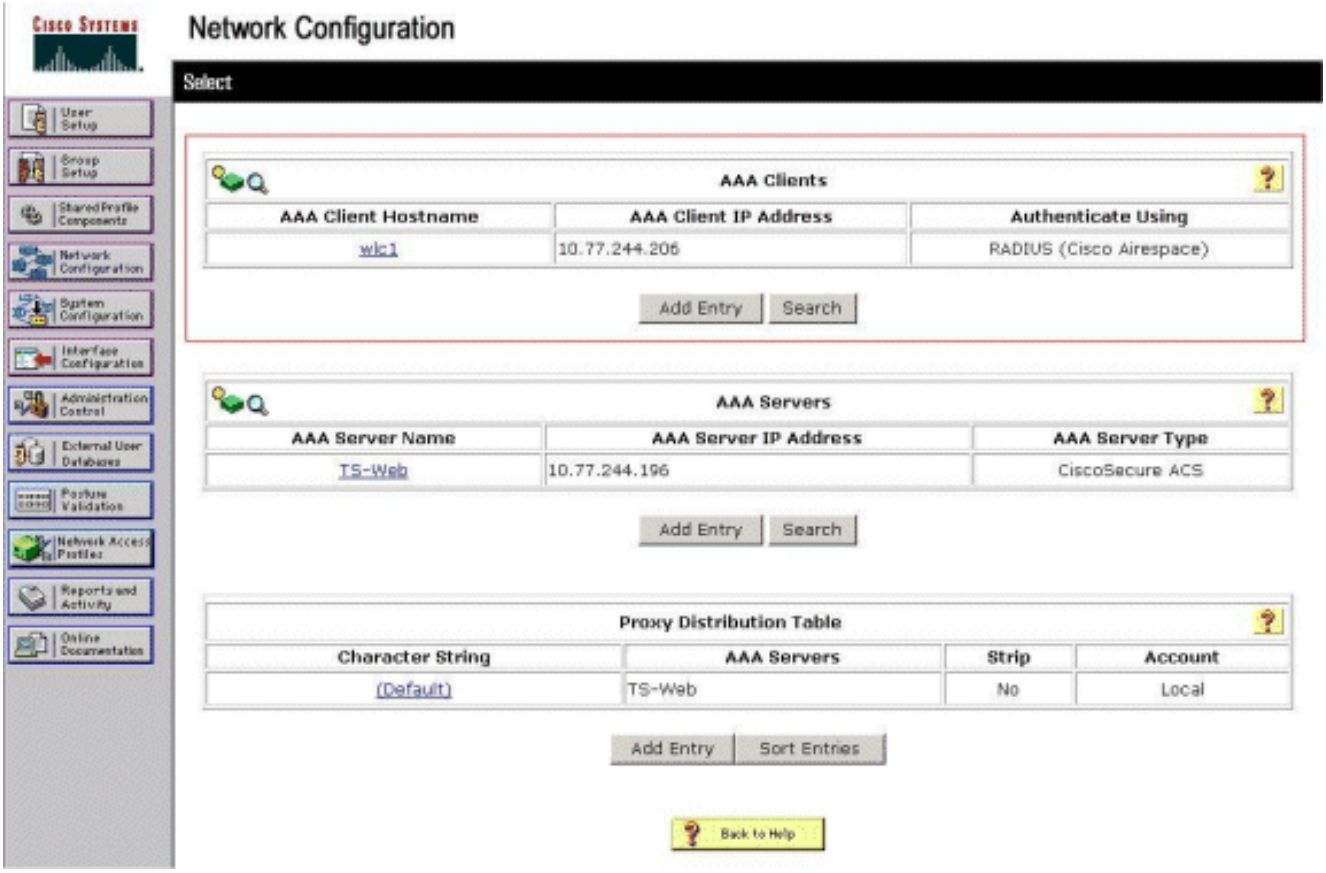
Проверьте ACS

1. Нажмите **User Setup**, и затем нажмите **List All Users** на GUI ACS.



Удостоверьтесь, что Статус Пользователя *Включен* и что Группа по умолчанию сопоставлена с пользователем.

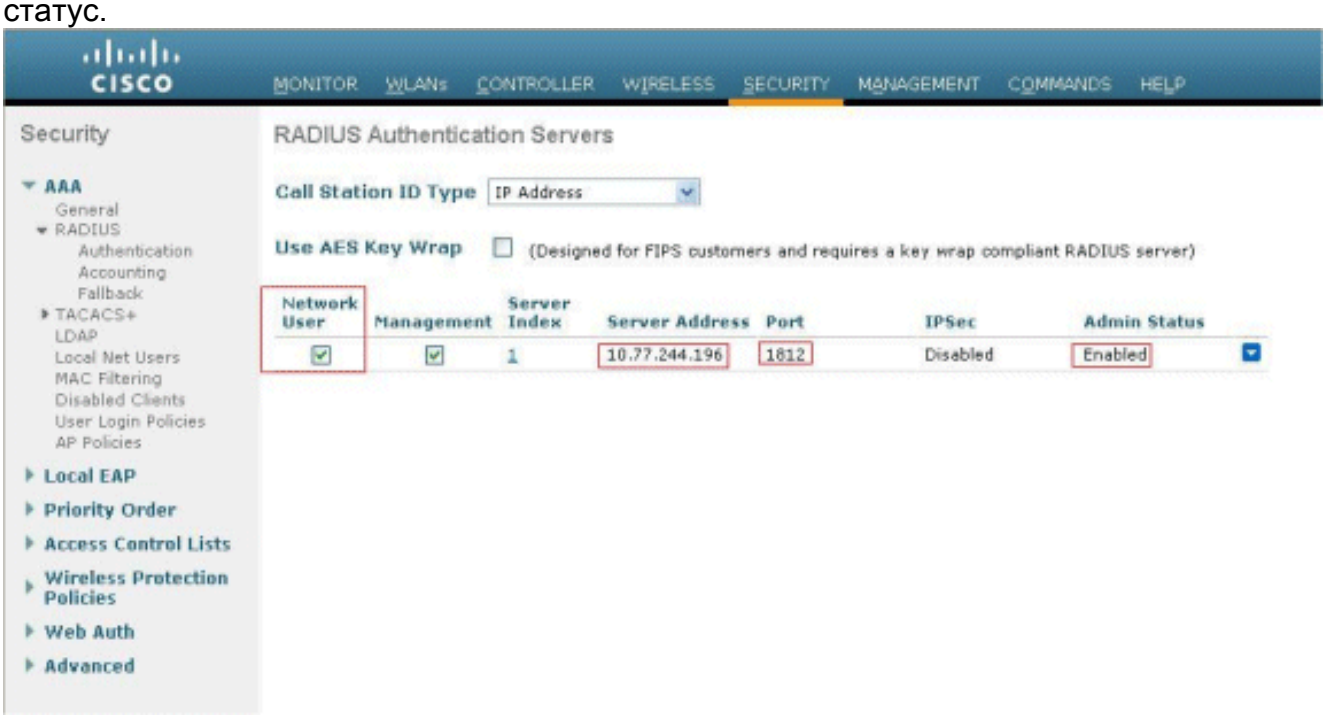
2. Нажмите вкладку **Network Configuration** и посмотрите в таблице **Клиентов AAA**, чтобы проверить, что WLC настроен как клиент AAA.



Проверьте WLC

1. Нажмите меню **WLAN** от GUI WLC.Удостоверьтесь, что WLAN, используемый для web-аутентификации, перечислен на странице.Удостоверьтесь, *что Включен* Административный статус для WLAN.Удостоверьтесь, что Политика безопасности для WLAN показывает *Веб-Аутентификацию*.

2. Нажмите **МЕНЮ СИСТЕМЫ БЕЗОПАСНОСТИ** от GUI WLC.Удостоверьтесь, что Cisco Secure ACS (10.77.244.196) перечислен на странице.Удостоверьтесь, что установлен флажок Пользователя сети.Удостоверьтесь, что порт является *1812* и что *Включен* Административный
статус.



Устранение неполадок

Существует много причин, почему web-аутентификация не успешна. Документ, Устраняющий неполадки Web-аутентификации на Контроллере беспроводной локальной сети (WLC) ясно, объясняет те причины подробно.

Команды для устранения неполадок

Примечание: См. раздел Важные сведения о командах отладки перед использованием этих **команд отладки**.

Telnet в WLC и выполняет эти команды для устранения проблем аутентификации:

- **debug aaa all enable**
```
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Successful transmission of
Authentic
ation Packet (id 1) to 10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:01
Fri Sep 24 13:59:52 2010: 00000000: 01 01 00 73 00 00 00 00  00 00 00 00 00 00 0
0 00  ...s............
Fri Sep 24 13:59:52 2010: 00000010: 00 00 00 00 01 07 75 73  65 72 31 02 12 93 c
3 66  ......user1....f
Fri Sep 24 13:59:52 2010: 00000030: 75 73 65 72 31
      user1
Fri Sep 24 13:59:52 2010: ****Enter processIncomingMessages: response code=2
Fri Sep 24 13:59:52 2010: ****Enter processRadiusResponse: response code=2
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Access-Accept received from RADIUS s
erver 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 0
Fri Sep 24 13:59:52 2010: AuthorizationResponse: 0x12238db0
Fri Sep 24 13:59:52 2010:       structureSize.............................89
Fri Sep 24 13:59:52 2010:       resultCode................................0
Fri Sep 24 13:59:52 2010:       protocolUsed..............................0x0
```

```
0000001
Fri Sep 24 13:59:52 2010:       proxyState.....................................00:
40:96:AC:DD:05-00:00
Fri Sep 24 13:59:52 2010:       Packet contains 2 AVPs:
Fri Sep 24 13:59:52 2010:           AVP[01] Framed-IP-Address..................
.....0xffffffff (-1) (4 bytes)
Fri Sep 24 13:59:52 2010:           AVP[02] Class..............................
.....CACS:0/5183/a4df4ce/user1 (25 bytes)
Fri Sep 24 13:59:52 2010: Authentication failed for user1, Service Type: 0
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Applying new AAA override for statio
n 00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Override values for station 00:40:96
:ac:dd:05
                source: 48, valid bits: 0x1
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                                vlanIfName: '',
aclName:
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Unable to apply override policy for
station 00:40:96:ac:dd:05 - VapAllowRadiusOverride is FALSE
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Sending Accounting request (0) for s
tation 00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: AccountingMessage Accounting Start: 0x1500501c
Fri Sep 24 13:59:52 2010:       Packet contains 12 AVPs:
Fri Sep 24 13:59:52 2010:           AVP[01] User-Name........................... .....user1
(5 bytes) Fri Sep 24 13:59:52 2010: AVP[02] Nas-Port.........................
.....0x00000002 (2) (4 bytes) Fri Sep 24 13:59:52 2010: AVP[03] Nas-Ip-
Address..................... .....0x0a4df4ce (172881102) (4 bytes) Fri Sep 24 13:59:52
2010: AVP[04] Framed-IP-Address.................. .....0x0a4df4c7 (172881095) (4 bytes)
```

- подробность debug aaa включает

Неудачные попытки аутентификации перечислены в меню, расположенном в Отчётах и Действии> Неудачные попытки.

Дополнительные сведения

- Пример настройки веб-аутентификации контроллера беспроводной LAN
- Устранение проблем web-аутентификации на контроллере беспроводной локальной сети (WLC)
- Пример настройки контроллера беспроводной сети с внешней веб-аутентификацией
- Пример конфигурации веб-проверки подлинности с использованием LDAP в контроллерах беспроводной LAN (WLC)
- Cisco Systems – техническая поддержка и документация