Пример настройки защищенного доступа по протоколу Wi-Fi (WPA 2)

Содержание

Введение

В настоящем документе описываются преимущества использования защищенного доступа Wi-Fi 2 (WPA 2) в беспроводных LAN (WLAN). Документ содержит два примера настройки WPA 2 на WLAN. Первый пример демонстрирует настройку WPA 2 в корпоративном режиме, а второй – настройку WPA 2 в частном режиме.

Примечание: WPA работает с Протоколом EAP.

Предварительные условия

Требования

Прежде чем выполнить данную конфигурацию, убедитесь, что вы обладаете базовыми

знаниями по следующим разделам:

- WPA
- Решения для безопасности беспроводных сетей**Примечание:** См. Общие сведения по обеспечению безопасности Cisco Aironet Wireless LAN для получения информации о решениях для безопасности беспроводных сетей Cisco.

Используемые компоненты

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

- Cisco Aironet 1310G Точка доступа (AP) / Мост, который выполняет релиз 12.3 программного обеспечения Cisco IOS (2) JA
- Aironet 802.11a/b/g Клиентский адаптер CB21AG, который выполняет микропрограммное обеспечение 2.5
- Служебная программа рабочего стола Aironet (ADU), которая выполняет микропрограммное обеспечение 2.5

Примечание: CB21AG Aironet и программное обеспечение клиентского адаптера PI21AG несовместимы с другим программным обеспечением Клиентского адаптера Aironet. Необходимо использовать ADU с платами CB21AG и PI21AG, а также Aironet Client Utility (ACU) всех других клиентских адаптеров Aironet. Для получения дополнительной информации о том, как настроить плату CB21AG и ADU, обратитесь к документу Установка клиентского адаптера.

Примечание: Этот документ использует AP/мост, который имеет интегрированную антенну. Если вы используете точку доступа или мост, требующие установки внешней антенны, необходимо убедиться в том, что антенны подключены к точке доступа или мосту. Иначе точка доступа или мост не сможет подключиться к беспроводной сети. Некоторые модели точек доступа и мостов производятся со встроенными антеннами, в то время как другим нужна для работы внешняя антенна. Для получения информации о том, какие модели точек доступа и мостов поставляются с встроенными, а какие с внешними антеннами, обратитесь к руководству по заказу/руководству по продукту соответствующего устройства.

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

WPA – это стандартный способ обеспечения безопасности Wi-Fi Alliance, учитывающий уязвимые места в сетях WLAN. WPA обеспечивает улучшенную защиту данных и контроль доступа к системам WLAN. WPA учитывает все известные уязвимые места протокола шифрования в беспроводной связи (WEP) исходного механизма обеспечения безопасности

IEEE 802.11 и обеспечивает безопасность сетей WLAN на предприятиях, в домашних сетях и небольших компаниях.

WPA 2 – это следующее поколение систем безопасности Wi-Fi. WPA 2 – это совместимая с Wi-Fi Alliance улучшенная версия одобренного стандарта IEEE 802.11i. WPA 2 выполнен на основе рекомендованного Национальным институтом стандартов и технологий (NIST) алгоритма шифрования AES (улучшенного стандарта шифрования) с использованием режима счетчика и протокола CCMP. Режим счетчика AES – это блочный шрифт, за раз шифрующий 128 битовый блок данных при помощи 128 битового ключа шифрования. Алгоритм CCMP генерирует код целостности сообщений (MIC), обеспечивающий беспроводному фрейму проверку подлинности происхождения данных и целостность данных.

Примечание: CCMP также упоминается как MAC CBC.

WPA 2 предлагает более высокий уровень безопасности, чем WPA, так как AES обеспечивает более стойкое шифрование, нежели протокол TKIP. TKIP – это протокол шифрования, используемый WPA. WPA 2 создает новые ключи сеанса при каждом сопоставлении. Ключи шифрования, используемые для каждого клиента сети, являются уникальными для этого клиента. В итоге каждый пакет, посылаемый в эфир, зашифрован при помощи уникального ключа. Система безопасности улучшена использованием нового и уникального ключа шифрования, так как повторно ключ не используется. WPA все еще считается безопасным, а протокол TKIP не был взломан. Тем не менее, Cisco рекомендует своим клиентам как можно скорее перейти на WPA 2.

WPA и WPA 2 поддерживают два режима работы:

- Расширенный режим
- Персональный режим

Этот документ обсуждает реализацию этих двух режимов с WPA 2.

Поддержка WPA 2 с оборудованием CISCO Aironet

WPA 2 поддерживается на этом оборудовании:

- Aironet 1130AG серия AP и 1230AG серия AP
- Серия Aironet 1100 AP
- Серия Aironet 1200 AP
- Серия Aironet 1300 AP

Примечание: Оборудуйте эти AP радио 802.11g и используйте программное обеспечение Cisco IOS версии 12.3 (2) JA или позже.

WPA 2 и AES поддерживаются также на:

- Радио модулях серии Aironet 1200 с шифрами компонента AIR-RM21A и AIR-RM22A**Примечание:** Aironet радио-модуль 1200 года с AIR-RM20A номера изделия не поддерживает WPA 2.
- Клиентских адаптерах Aironet 802.11a/b/g, использующих микропрограмму 2.5

Примечание: Продукты Cisco Aironet серии 350 не поддерживают WPA 2, потому что их радио испытывают недостаток в поддержке AES.

Примечание: Беспроводные мосты Cisco Aironet серии 1400 не поддерживают WPA 2 или AES.

Настройка в режиме enterprise

Термин режим enterprise относится к продуктам, имеющим возможность взаимодействия с режимами работы аутентификации Pre-Shared Key (PSK) и IEEE 802.1x. Режим 802.1x считается более безопасным, чем любая другая существующая инфраструктура аутентификации, благодаря своей гибкости в поддержке разнообразных механизмов аутентификации и стойким алгоритмам шифрования. WPA 2 в режиме enterprise осуществляет аутентификацию в два этапа. В первой фазе происходит настройка открытой аутентификации. Во второй фазе происходит аутентификация 802.1x с одним из методов EAP. AES обеспечивает механизм шифрования.

В режиме enterprise клиенты и сервера аутентификации подтверждают подлинность друг друга при помощи метода аутентификации EAP, а затем и клиент и сервер генерируют PMK (Pairwise Master Key). При использовании WPA 2 сервер динамически генерирует PMK и передает его на точку доступа.

В данном разделе рассматривается настройка, необходимая для реализации WPA 2 в режиме работы enterprise.

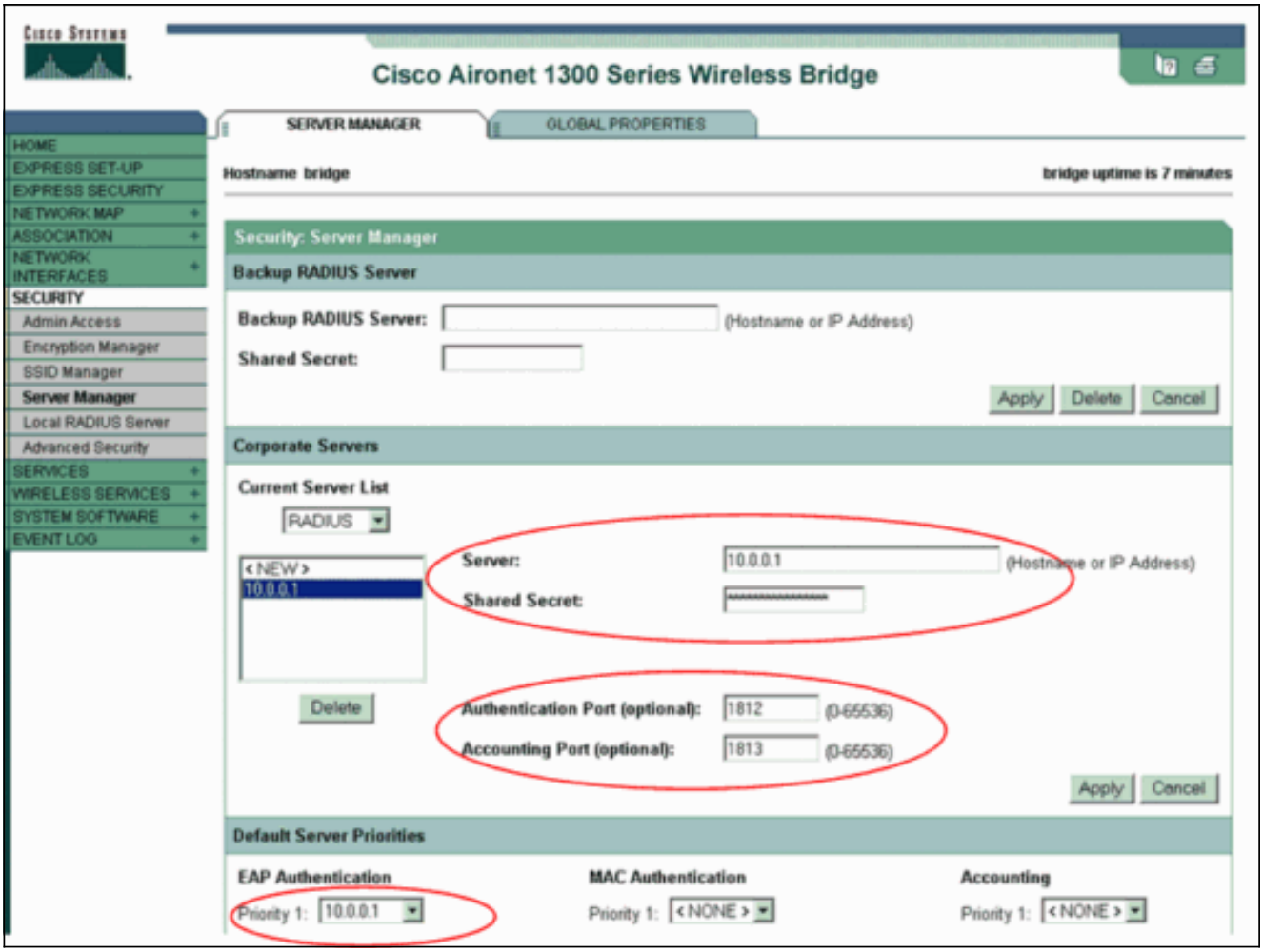
Настройка сети

В этой настройке Aironet 1310G AP/мост, который выполняет Расширяемый протокол аутентификации облегченного Cisco (LEAP), аутентифицирует пользователя с адаптером 2 совместимых клиентов WPA. Управление ключами происходит при помощи WPA 2, для которого настроено шифрование AES-CCMP. Точка доступа настроена как локальный RADIUS сервер, выполняющий LEAP аутентификацию. Для реализации этой настройки необходимо настроить клиентский адаптер и точку доступа. Разделы Настройка точки доступа и Настройка клиентского адаптера описывают настройку точки доступа и клиентского адаптера.

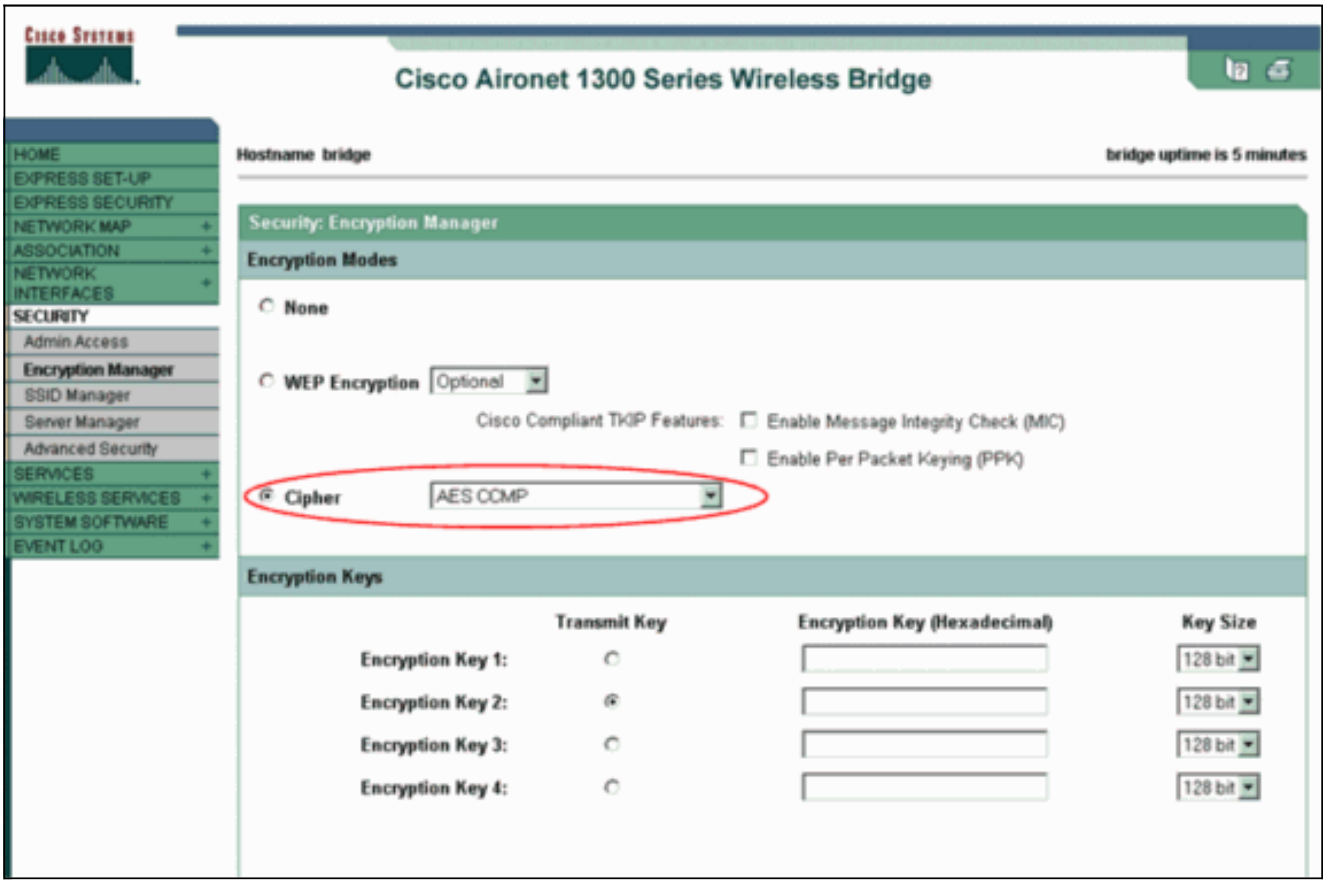
Настройте AP

Выполните эти шаги для настройки AP с помощью GUI:

1. Настроить точку доступа как локальный RADIUS сервер, выполняющий LEAP аутентификацию.Выберите **Security> Server Manager** в меню слева и определите IP-адрес, порты и общий секретный ключ сервера RADIUS.Так как при данной конфигурации точка доступа настроена как RADIUS сервер, нужно использовать IP адрес точки доступа. Для работы локального RADIUS сервера необходимо использовать порты 1812 и 1813.В зоне Default Server Priorities определить приоритет EAP аутентификации по умолчанию как 10.0.0.1.**Примечание:** 10.0.0.1 локальный сервер
RADIUS.

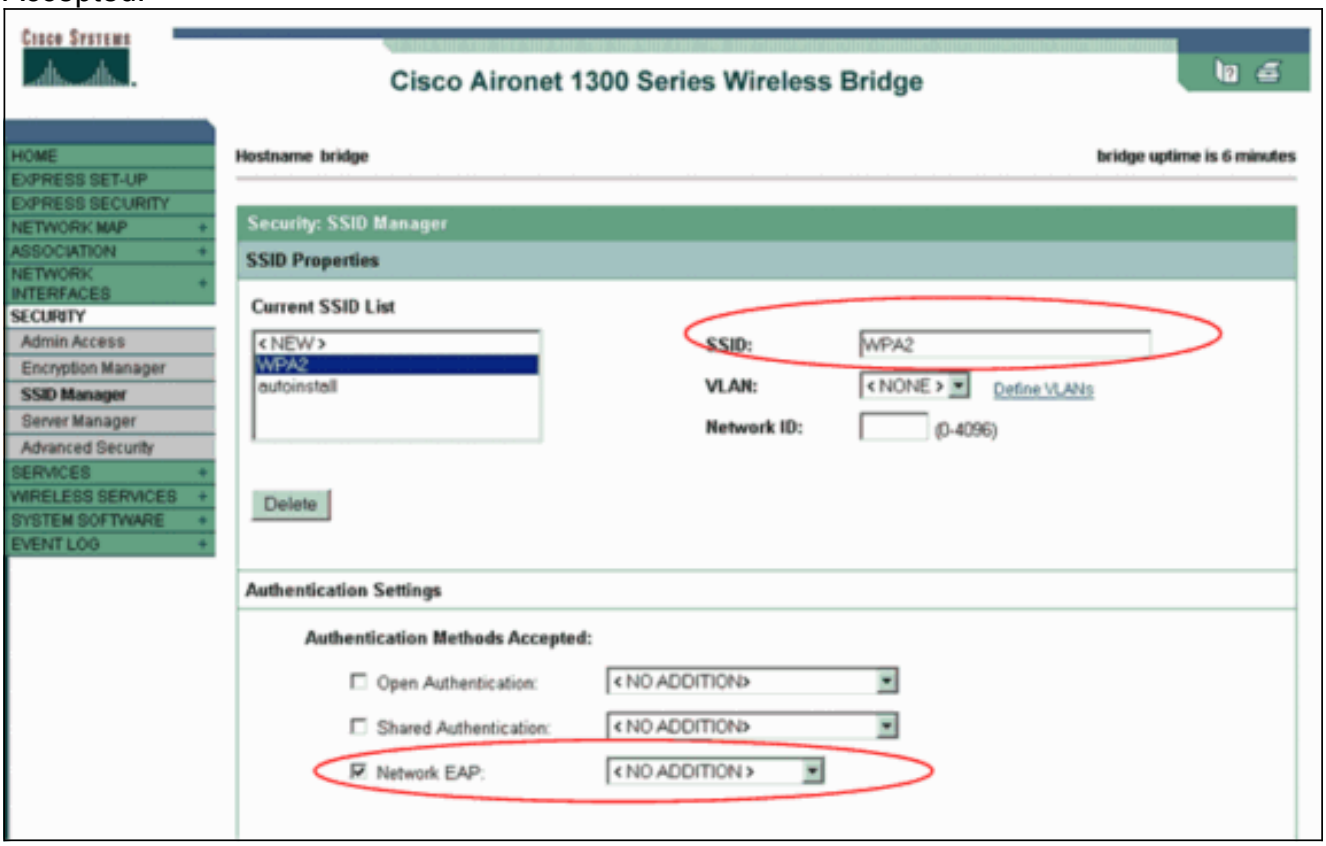


2. Выберите **Security> Encryption Manager** из меню слева и выполните эти шаги:**Из меню Cipher, выбрать AES CCMP.**Это действие включает AES шифрование с использованием режима счетчика с CBC-MAC.



Щелкните "Применить".

3. Выберите **Security> SSID Manager** и создайте новые идентификаторы наборов сервисов (SSID) для использования с WPA 2.Проверьте флажок **Network EAP** в области Authentication Methods
Accepted.

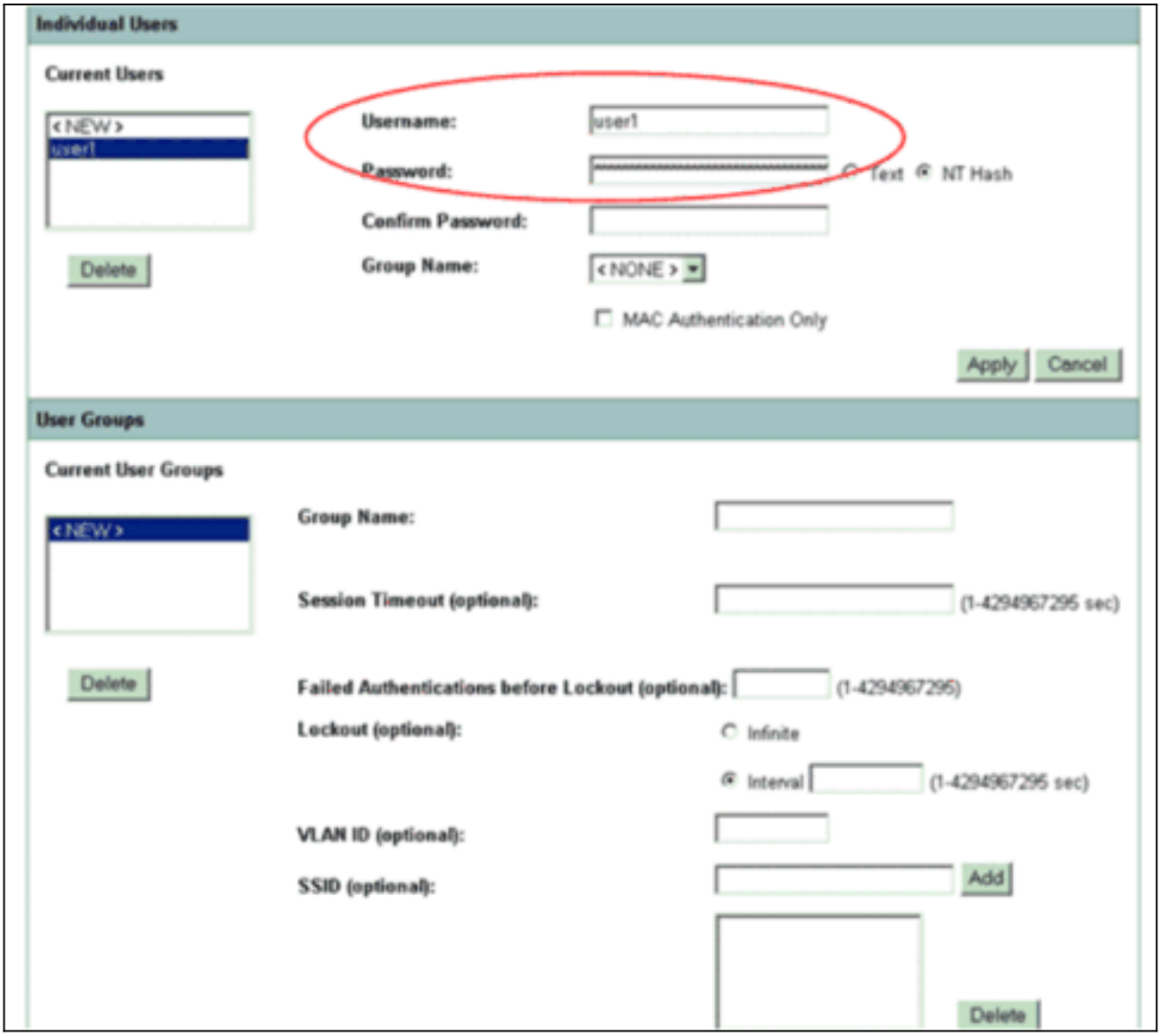


Примечание: Используйте эти рекомендации при настройке типа проверки подлинности на радиоинтерфейсе:Клиенты Cisco - используют сетевой расширенный протокол аутентификации (EAP).Клиентами стороннего производителя (включая продукты, совместимые с CCX [разрешения, совместимые с Cisco]) должна использоваться открытая аутентификация с EAP.Использующим сочетание клиентских устройств Cisco и сторонних производителей необходимо выбрать и сетевой EAP и открытую аутентификацию с EAP.Выполнить прокрутку вниз окна Security SSID Manager до зоны Authenticated Key Management и выполнить следующие действия:**Из меню Key Management, выбрать Mandatory.Установить флажок WPA справа.Щелкните "Применить".Примечание:** Определение VLAN является дополнительным. Если VLAN будет определена, то клиентские устройства, связанные с использованием данного SSID, сгруппируются в VLAN. Для получения дополнительной информации о реализации VLAN см. раздел Настройка
VLAN.

4. Выберите **Security> Local Radius Server** и выполните эти шаги:**Нажать на закладку General Set-Up, расположенную вверху окна.Установить флажок LEAP и нажать Apply.**В зоне Network Access Servers определить IP адрес и общий секретный ключ RADIUS сервера.Для локального RADIUS сервера необходимо использовать IP-адрес точки доступа.

Щелкните "Применить".

5. Выполнить прокрутку вниз окна General Set-Up до зоны Individual Users и определить индивидуальных пользователей.Определение групп пользователей является необязательным.



Такая конфигурация определяет пользователя с именем "user1" и пароль. Также конфигурация выбирает NT хеш для пароля. После выполнения процедуры, описанной в данном разделе, точка доступа готова принимать запросы на аутентификацию от клиентов. Следующим шагом является настройка клиентского адаптера.

Конфигурация интерфейса командой строки CLI

Точка доступа
ap#**show running-config** Building configuration... . . . **aaa new-model** *!--- This command reinitializes the authentication, !--- authorization and accounting functions.* ! ! **aaa group server radius rad_eap server 10.0.0.1 auth-port 1812 acct-port 1813** *!--- A server group for RADIUS is created called "rad_eap" !--- that uses the server at 10.0.0.1 on ports 1812 and 1813.* . . . **aaa authentication login eap_methods group rad_eap** *!--- Authentication [user validation] is to be done for !--- users in a group called "eap_methods" who use server group "rad_eap".* . . . ! bridge irb ! interface Dot11Radio0 no ip address no ip route-cache ! **encryption vlan 1 key 1 size 128bit 12345678901234567890123456 transmit-key** *!---This step is optional !--- This value seeds the initial key for use with !--- broadcast [255.255.255.255] traffic. If more than one VLAN is !--- used, then keys must be set for each VLAN.* **encryption**

```
vlan 1 mode wep mandatory !--- This defines the policy
for the use of Wired Equivalent Privacy (WEP). !--- If
more than one VLAN is used, !--- the policy must be set
to mandatory for each VLAN. broadcast-key vlan 1 change
300 !--- You can also enable Broadcast Key Rotation for
each vlan and Specify the time after which Brodacst key
is changed. If it is disabled Broadcast Key is still
used but not changed. ssid cisco vlan 1 !--- Create a
SSID Assign a vlan to this SSID authentication open eap
eap_methods authentication network-eap eap_methods !---
Expect that users who attach to SSID "cisco" !---
request authentication with the type 128 Open EAP and
Network EAP authentication !--- bit set in the headers
of those requests, and group those users into !--- a
group called "eap_methods." ! speed basic-1.0 basic-2.0
basic-5.5 basic-11.0 rts threshold 2312 channel 2437
station-role root bridge-group 1 bridge-group 1
subscriber-loop-control bridge-group 1 block-unknown-
source no bridge-group 1 source-learning no bridge-group
1 unicast-flooding bridge-group 1 spanning-disabled . .
. interface FastEthernet0 no ip address no ip route-
cache duplex auto speed auto bridge-group 1 no bridge-
group 1 source-learning bridge-group 1 spanning-disabled
! interface BVI1 ip address 10.0.0.1 255.255.255.0 !---
The address of this unit. no ip route-cache ! ip
default-gateway 10.77.244.194 ip http server ip http
help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server local !--- Engages the Local RADIUS Server
feature. nas 10.0.0.1 key shared_secret !--- Identifies
itself as a RADIUS server, reiterates !--- "localness"
and defines the key between the server (itself) and the
access point(itself). ! group testuser !--- Groups are
optional. ! user user1 nthash password1 group testuser
!--- Individual user user user2 nthash password2 group
testuser !--- Individual user !--- These individual
users comprise the Local Database ! radius-server host
10.0.0.1 auth-port 1812 acct-port 1813 key shared_secret
!--- Defines where the RADIUS server is and the key
between !--- the access point (itself) and the server.
radius-server retransmit 3 radius-server attribute 32
include-in-access-req format %h radius-server
authorization permit missing Service-Type radius-server
vsa send accounting bridge 1 route ip ! ! line con 0
line vty 5 15 ! end
```

Настройте клиентский адаптер

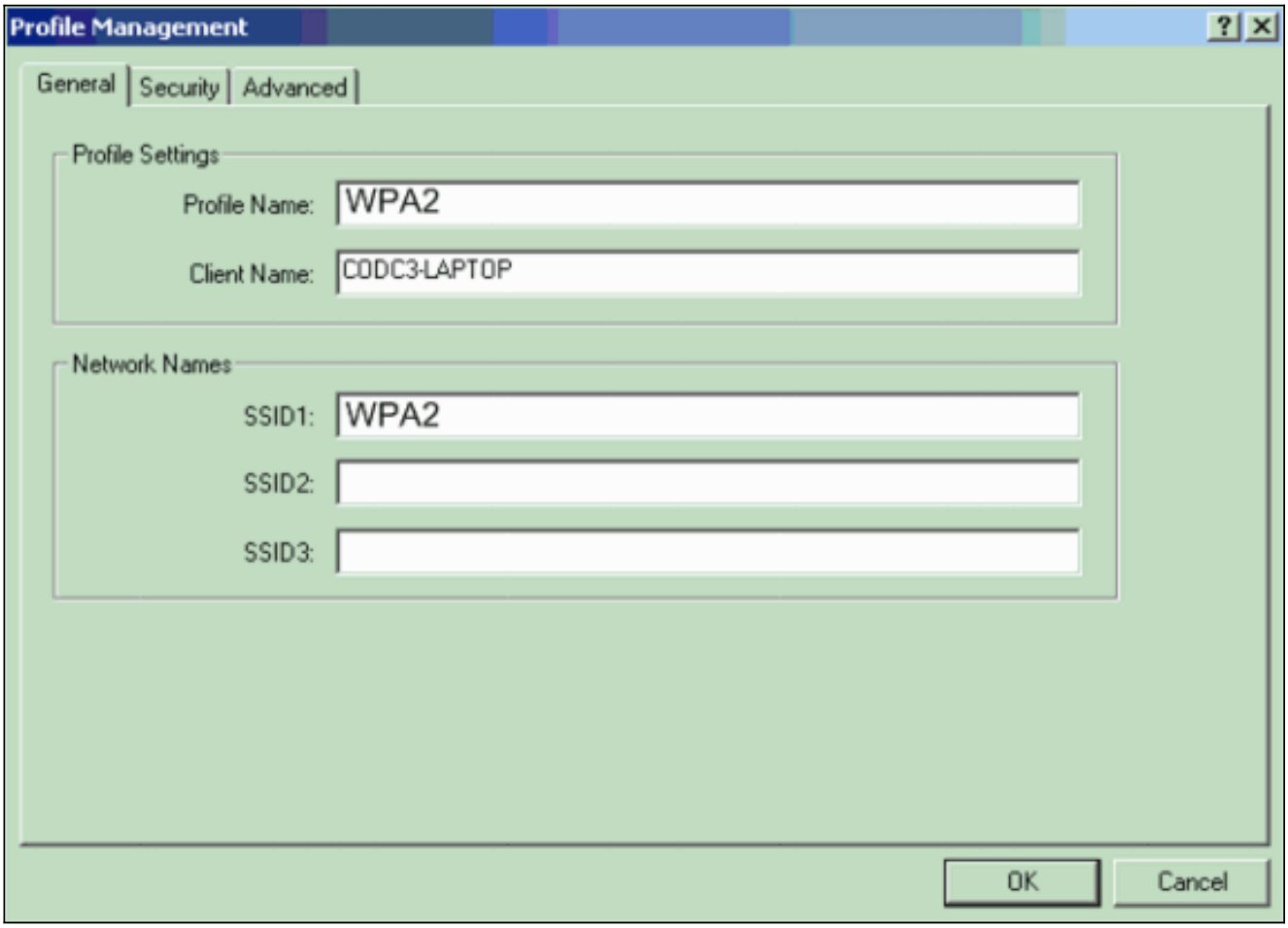
Выполните следующие действия:

Примечание: Этот документ использует Aironet 802.11a/b/g Клиентский адаптер, который выполняет микропрограммное обеспечение 2.5 и объясняет конфигурацию клиентского адаптера с версией ADU 2.5.

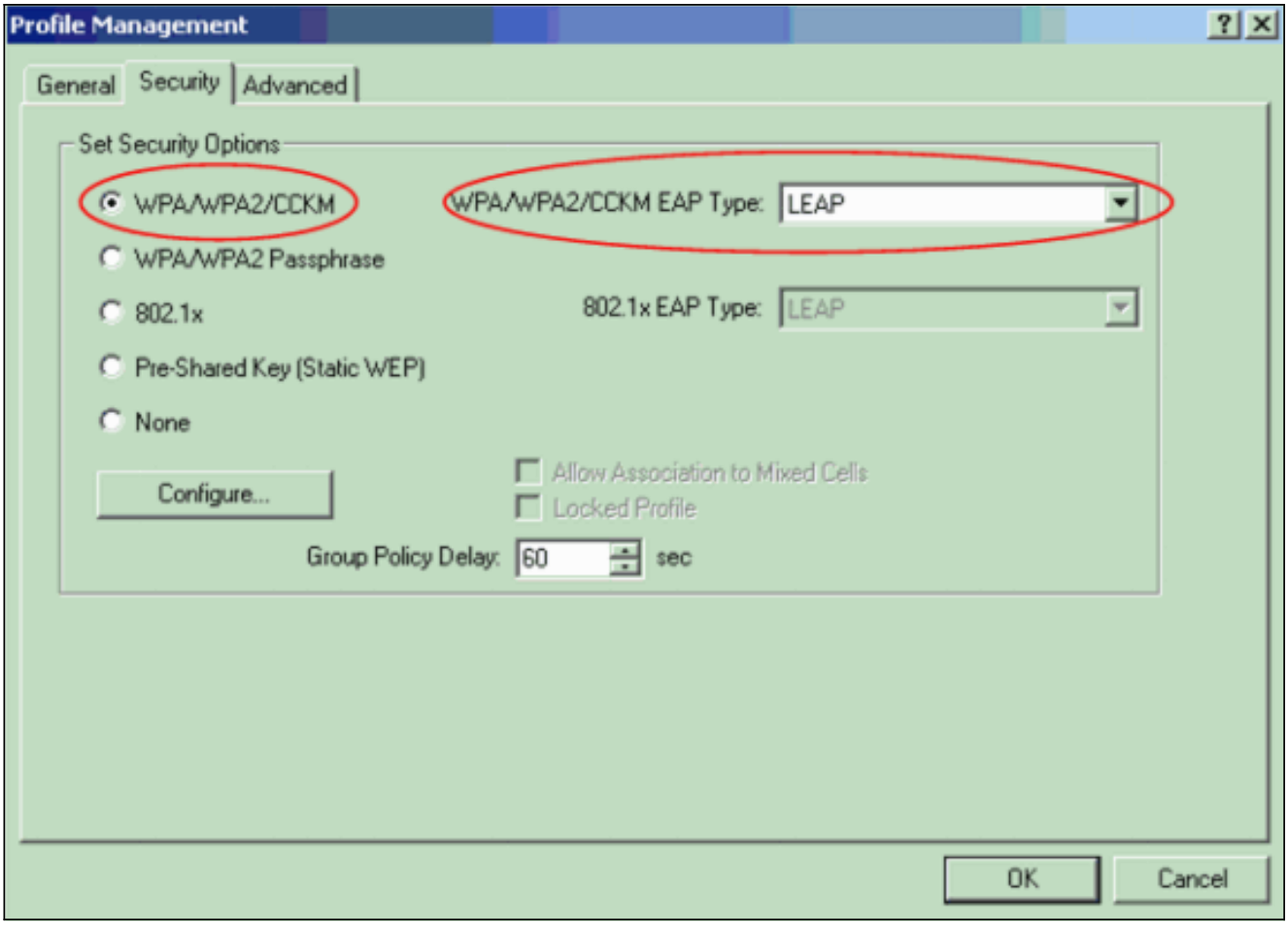
1. **В окне Profile Management на ADU необходимо нажать New, чтобы создать новый профиль.**Отобразится новое окно, в котором можно задать конфигурацию режима работы WPA 2 enterprise. На закладке General ввести имя профиля (Profile Name) и SSID, который будет использоваться клиентским адаптером.В этом примере именем

профиля и SSID является WPA2:**Примечание:** SSID должен совпасть с SSID, который вы настроили на AP для WPA

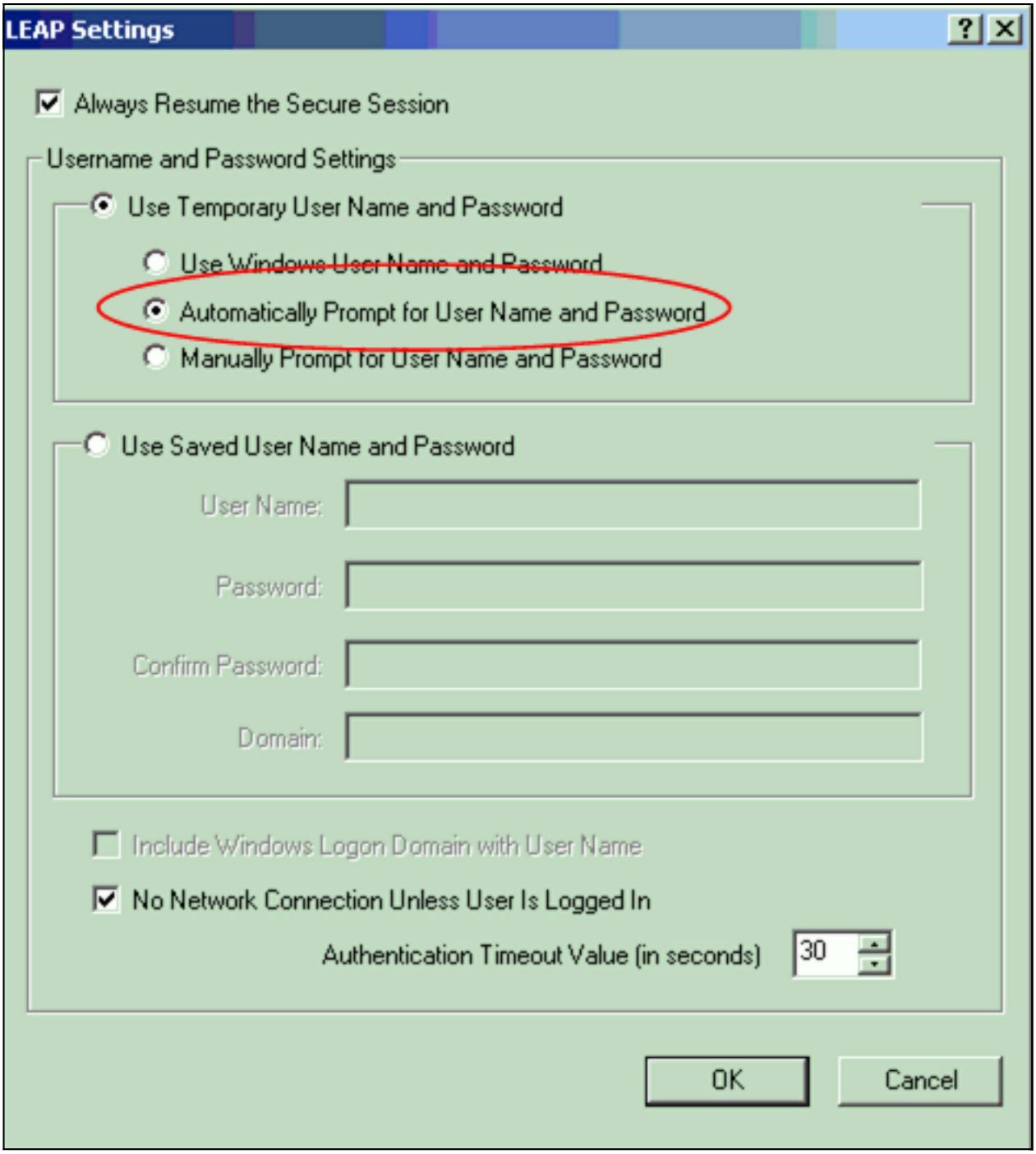
2.



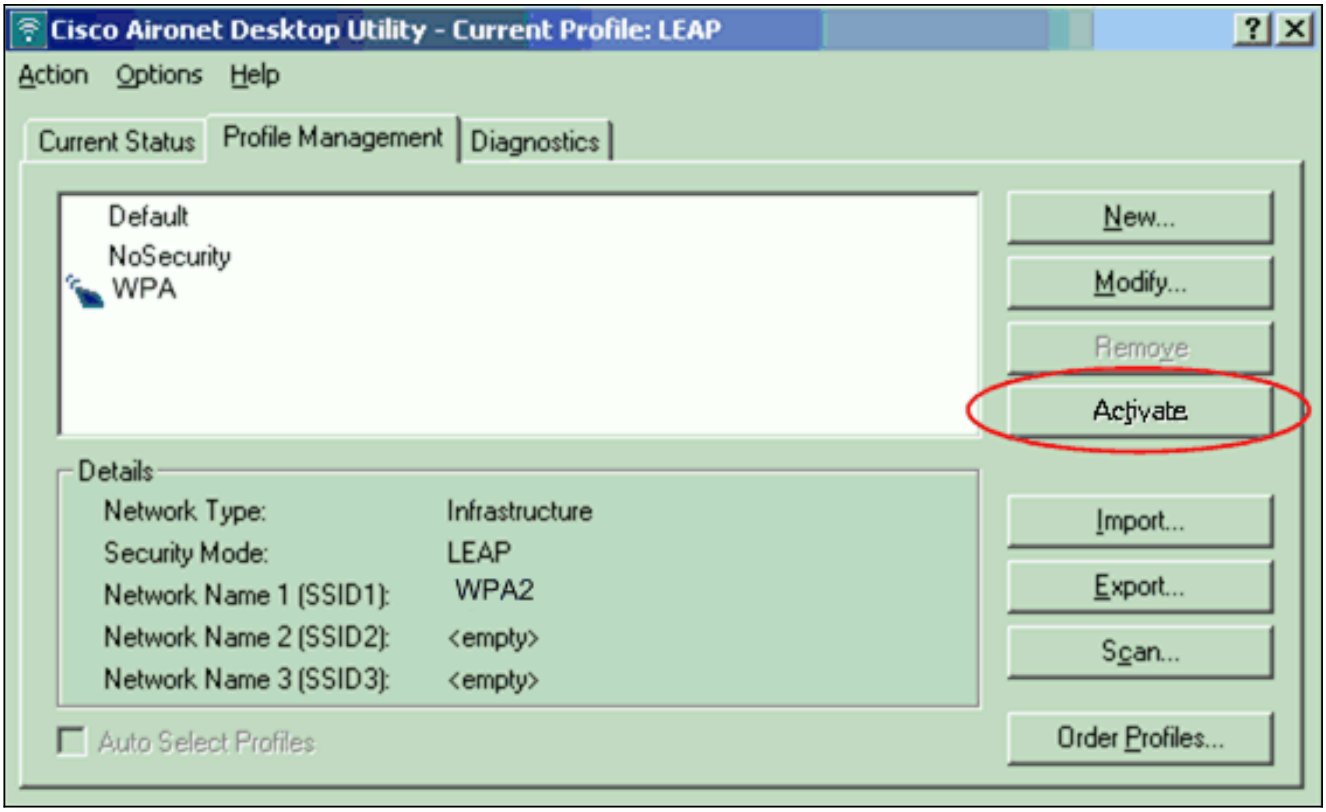
2. **Нажать на закладку Security, нажать WPA/WPA2/CCKMи выбрать LEAP из меню WPA/WPA2/CCKM EAP Type.**Это действие подключает WPA или WPA 2, в зависимости от того, что было настроено на точке
доступа.



3. **Нажать Configure для определения установок LEAP.**
4. **Выбрать на основании требований соответствующие имя пользователя (Username) и установки пароля (Password Settings) и нажать OK.**Даная конфигурация выбирает опцию Automatically Prompt для имени пользователя и пароля. Данный параметр позволяет вводить имя и пароль вручную при прохождении LEAP-аутентификации.



5. Нажать OK, чтобы выйти из окна Profile Management.
6. Нажать Activate, чтобы активировать этот профиль на клиентском адаптере.

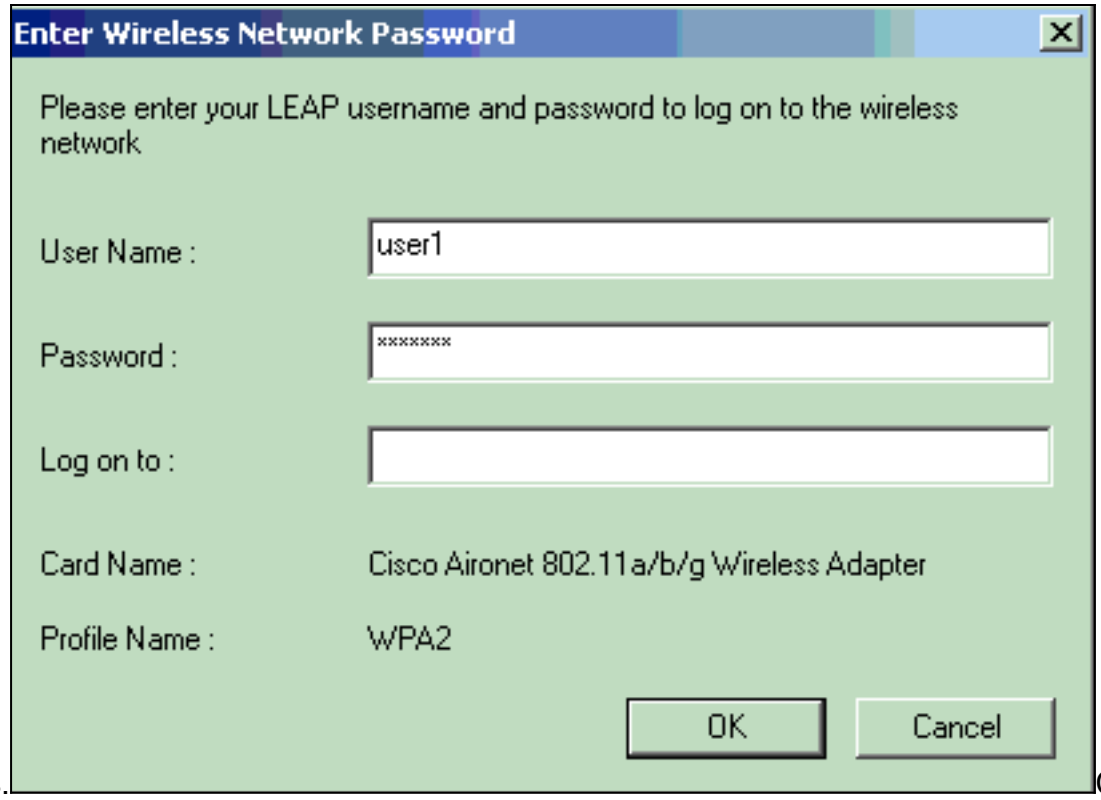


Примечание: При использовании Microsoft Wireless Zero Configuration (WZC) для настройки клиентского адаптера, по умолчанию, WPA 2 не доступен с WZC. Поэтому для того, чтобы позволить клиентам с включенной WZC использовать WPA 2, необходимо установить hot fix для Microsoft Windows XP. Для установки обратитесь к ресурсу Центр загрузки ПО Microsoft – Обновления для Windows XP (KB893357) .После установки hot fix можно настроить WPA 2 при использовании WZC.

Проверка

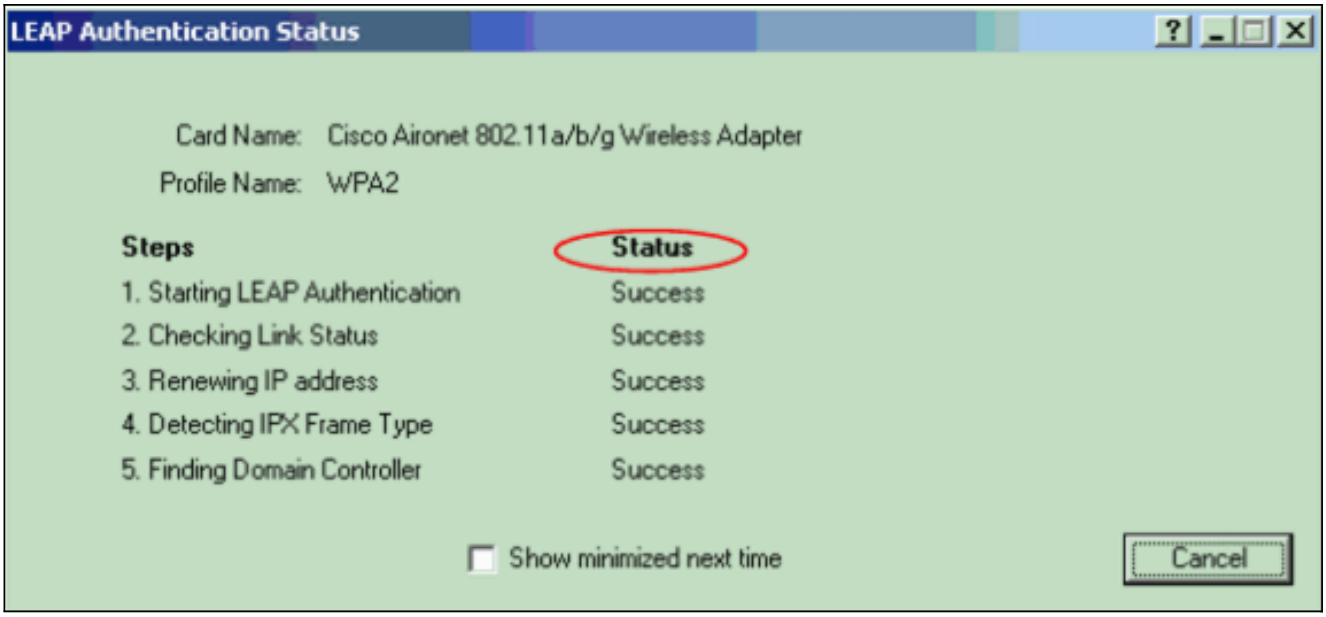
Этот раздел позволяет убедиться, что конфигурация работает правильно.

1. При отображении окна Enter Wireless Network Password введите имя пользователя и



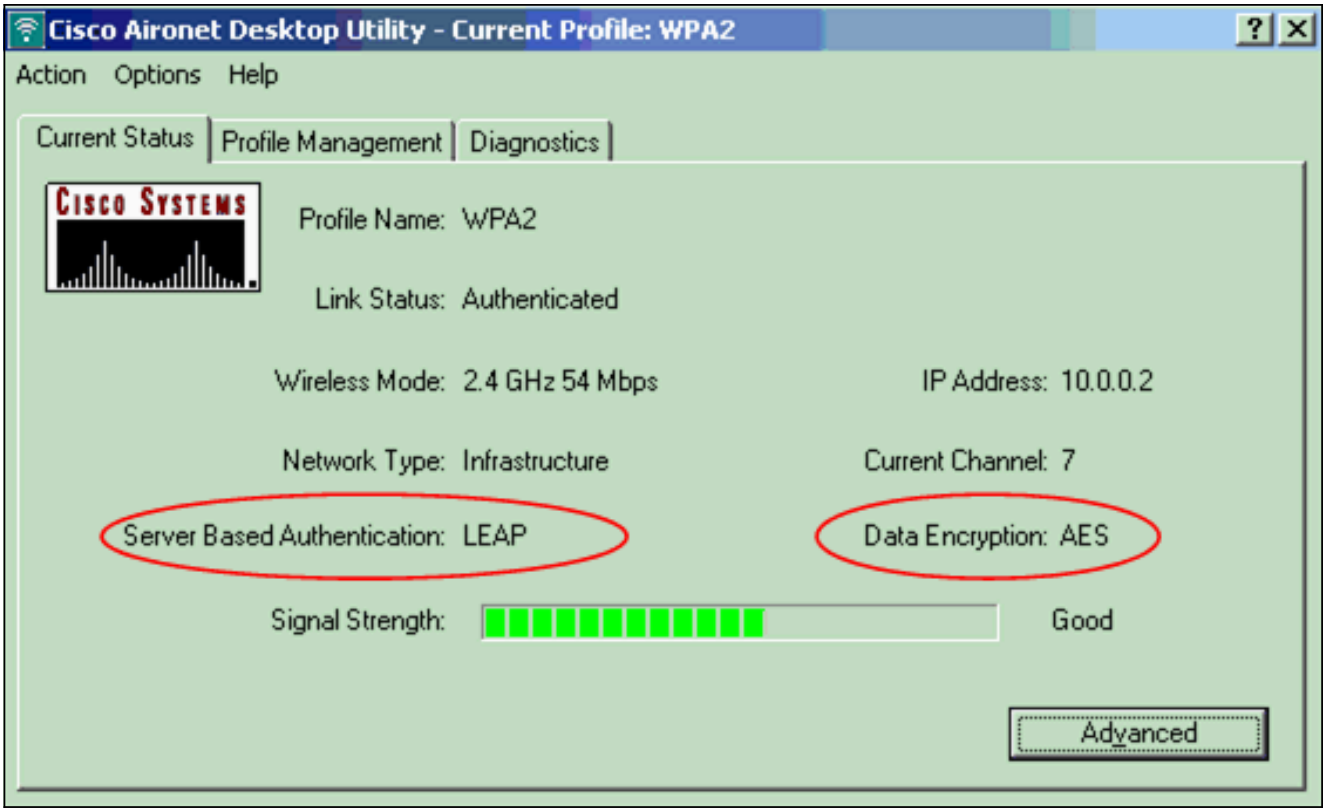
пароль. Следующее окно – LEAP Authentication Status. На этой фазе учетные записи пользователей проверяются на локальном RADIUS сервере.

2. Для того, чтобы увидеть результат аутентификации, необходимо проверить зону Status.



При успешном завершении аутентификации клиент подключится к беспроводной LAN.

3. Чтобы убедиться в том, что клиент использует AES шифрование и LEAP аутентификацию, необходимо проверить ADU Current Status.Это покажет, что в WLAN был реализован WPA 2 с LEAP аутентификацией и AES шифрованием.



4. Чтобы убедиться в том, что клиент успешно прошел аутентификацию при помощи WPA 2, необходимо проверить журнал событий точки доступа/моста.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Настройка в режиме personal

Термин режим personal относится к продуктам, имеющим возможность взаимодействия с режимом работы аутентификации PSK-only. Данный режим предполагает ручную настройку

PSK на точке доступа и клиенте. PSK аутентифицирует пользователей при помощи пароля или идентификационного кода на клиентской станции и на точке доступа. Сервер аутентификации не требуется. Клиент может получить доступ к сети только если пароль клиента соответствует паролю точки доступа. Пароль также обеспечивает ключевой материал, используемый TKIP или AES для генерации ключа шифрования для шифрования пакетов данных. Режим personal нацелен на среды SOHO, а также считается безопасным для сред предприятий. В данном разделе рассматривается настройка, необходимая для реализации WPA 2 в режиме работы personal.

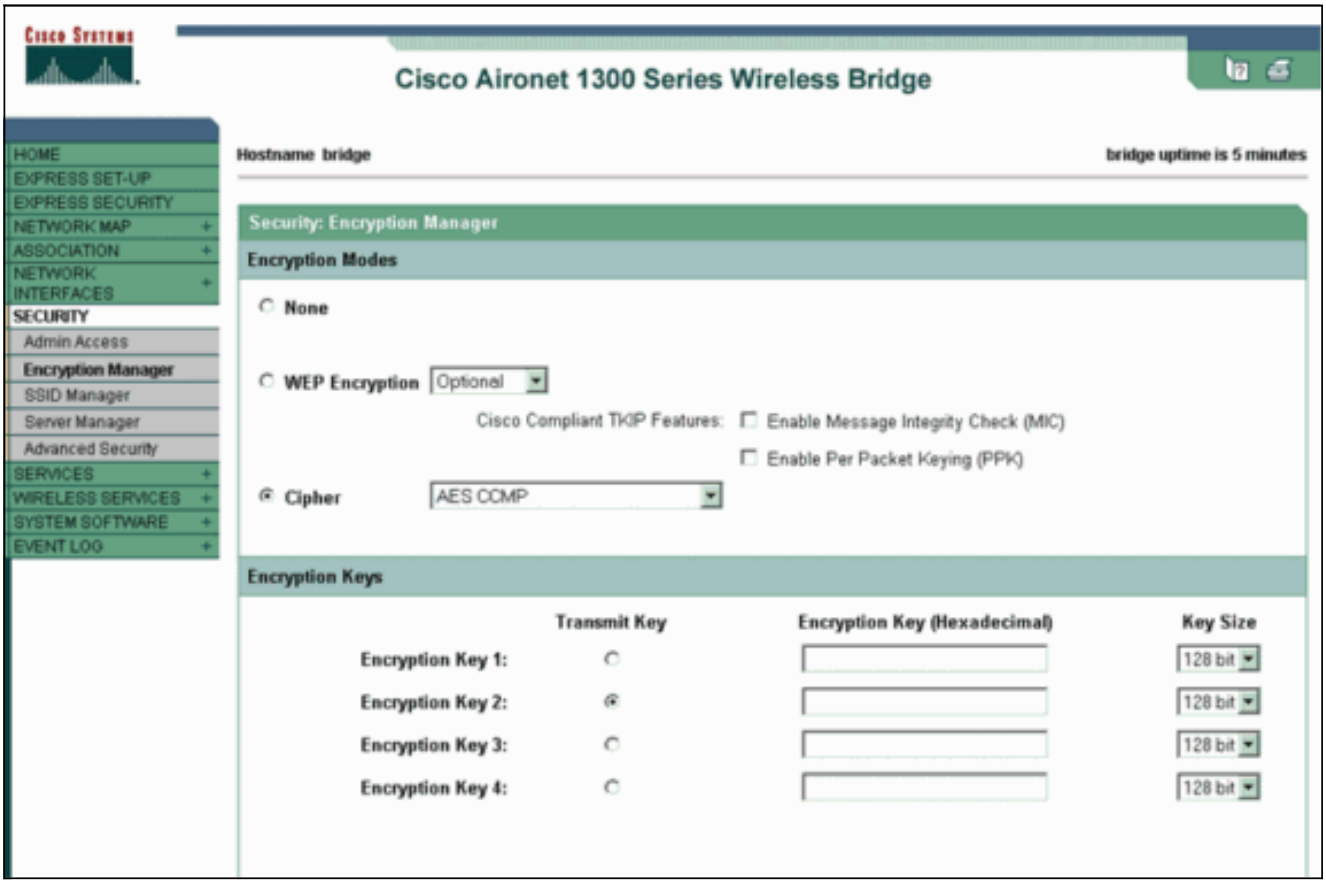
Настройка сети

В этой настройке пользователь с адаптером 2 совместимых клиентов WPA аутентифицируется на Aironet 1310G AP/мост. Управление ключами происходит при помощи WPA 2 PSK, для которого настроено шифрование AES-CCMP. Разделы Настройка точки доступа и Настройка клиентского адаптера описывают настройку точки доступа и клиентского адаптера.

Настройте AP

Выполните следующие действия:

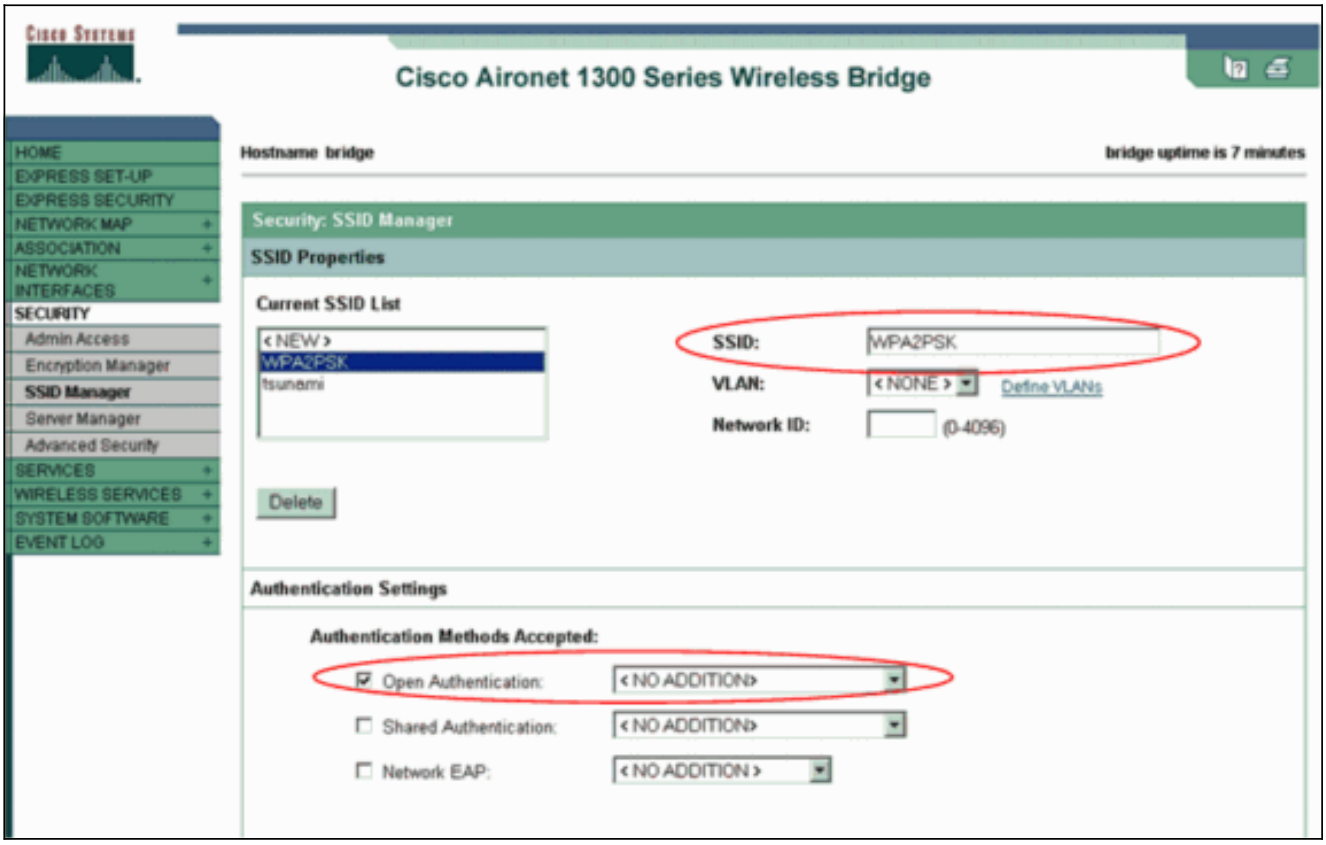
1. Выберите **Security> Encryption Manager** в меню слева и выполните эти шаги:**Из меню Cipher, выбрать AES CCMP.**Это действие включает AES шифрование с использованием режима счетчика с CCMP.



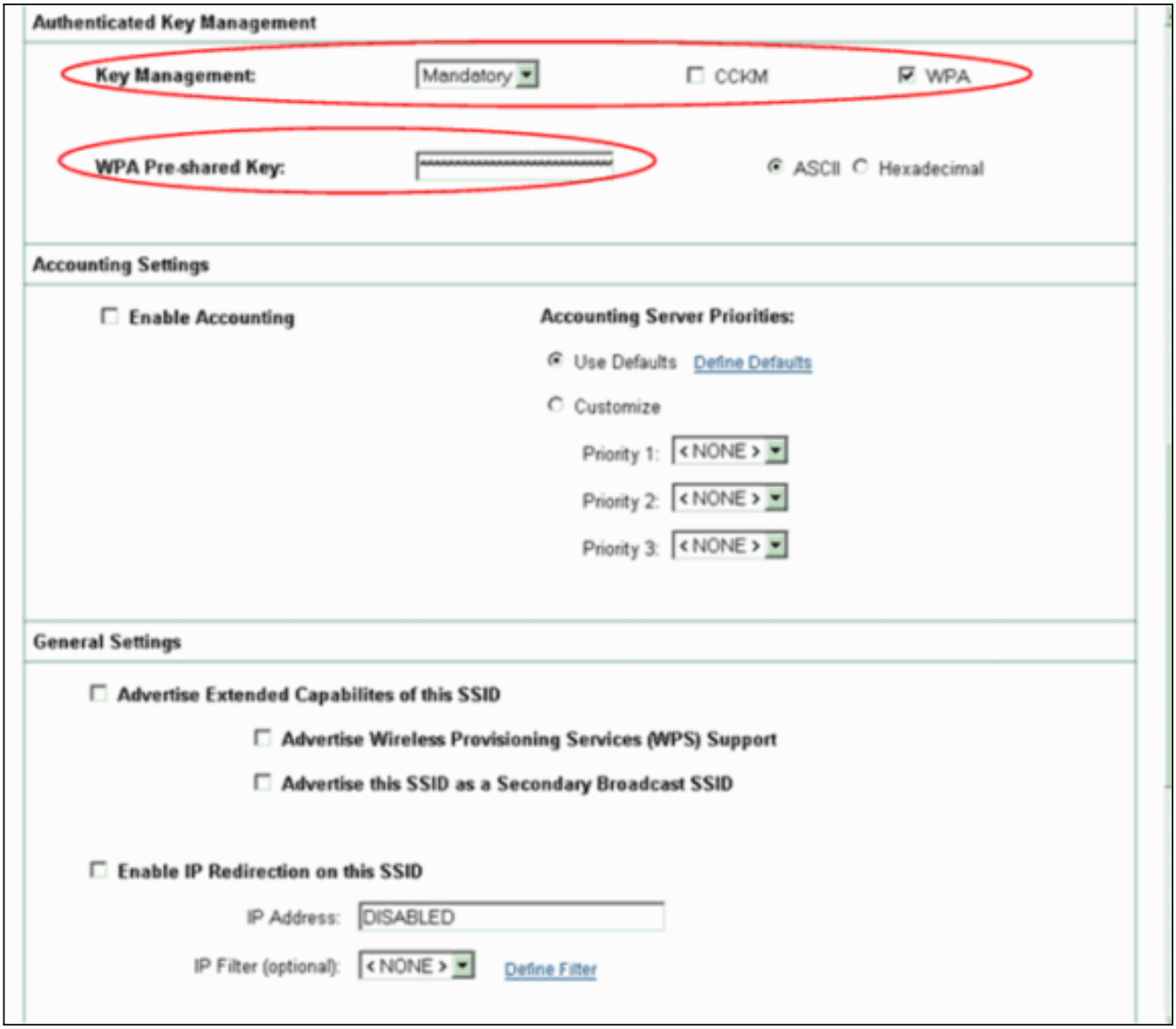
Щелкните "Применить".

2. Выберите **Security> SSID Manager** и создайте новый SSID для использования с WPA 2.**Установить флажок Open**

Authentication.



Выполнить прокрутку вниз окна Security SSID Manager до зоны Authenticated Key Management и выполнить следующие действия:**Из меню Key Management, выбрать Mandatory.Установить флажок WPA**
справа.



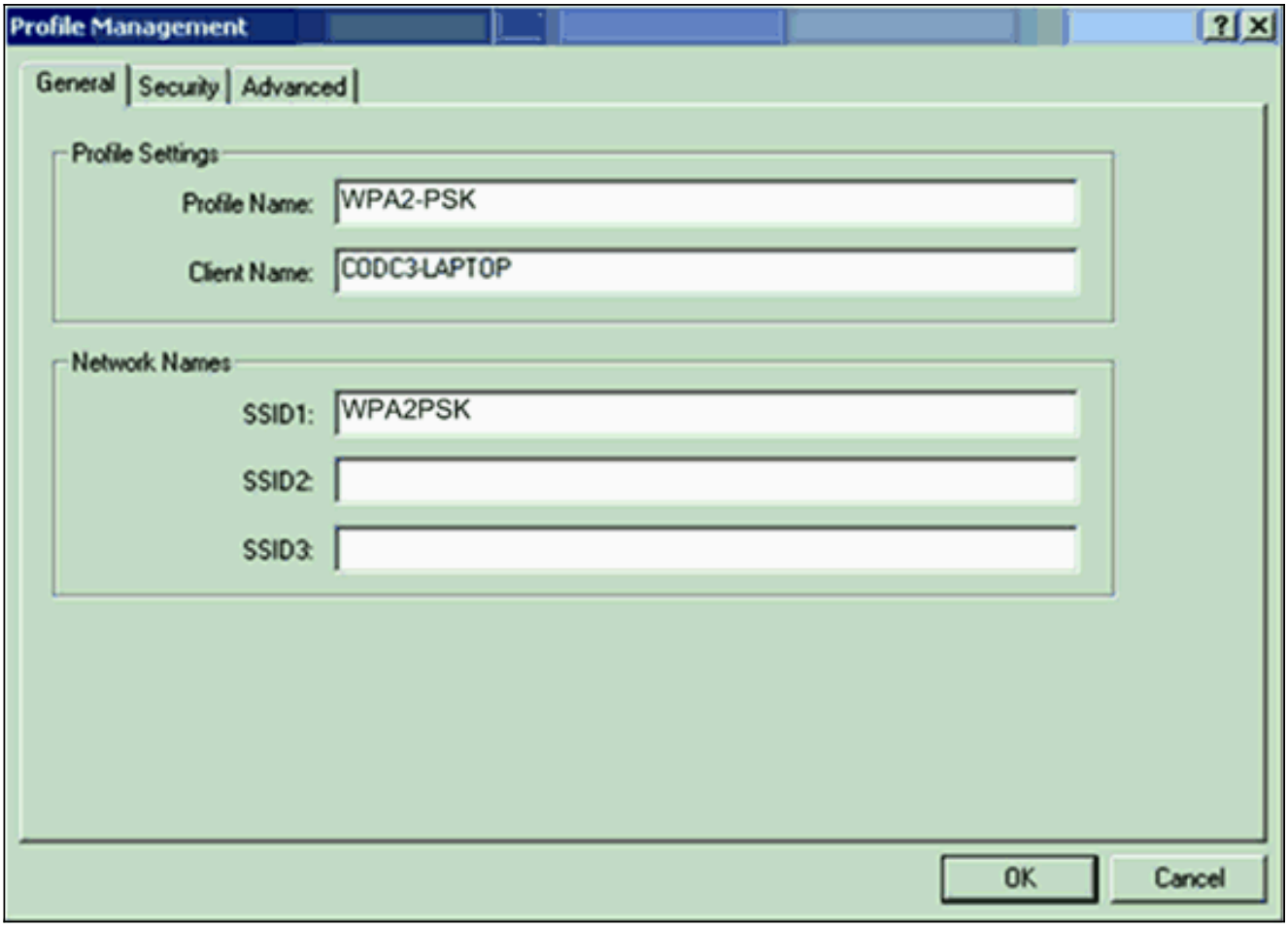
Ввести общий секретный ключ WPA PSK или ключ идентификационной фразы WPA PSK.Этот ключ должен соответствовать ключу WPA PSK, настроенному на клиентском адаптере.**Щелкните "Применить".**

Теперь точка доступа может получать запросы на аутентификацию от беспроводных клиентов.

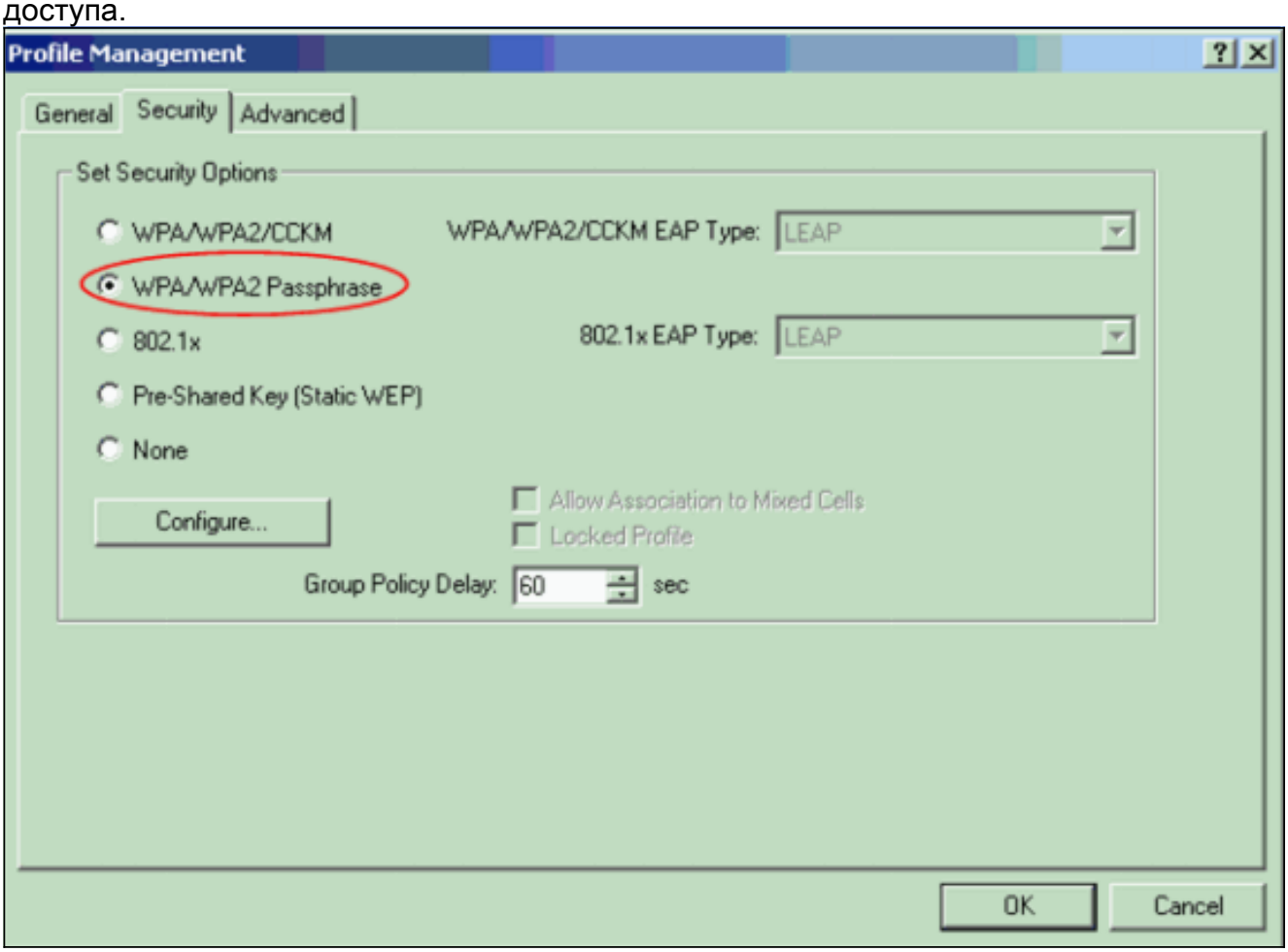
Настройте клиентский адаптер

Выполните следующие действия:

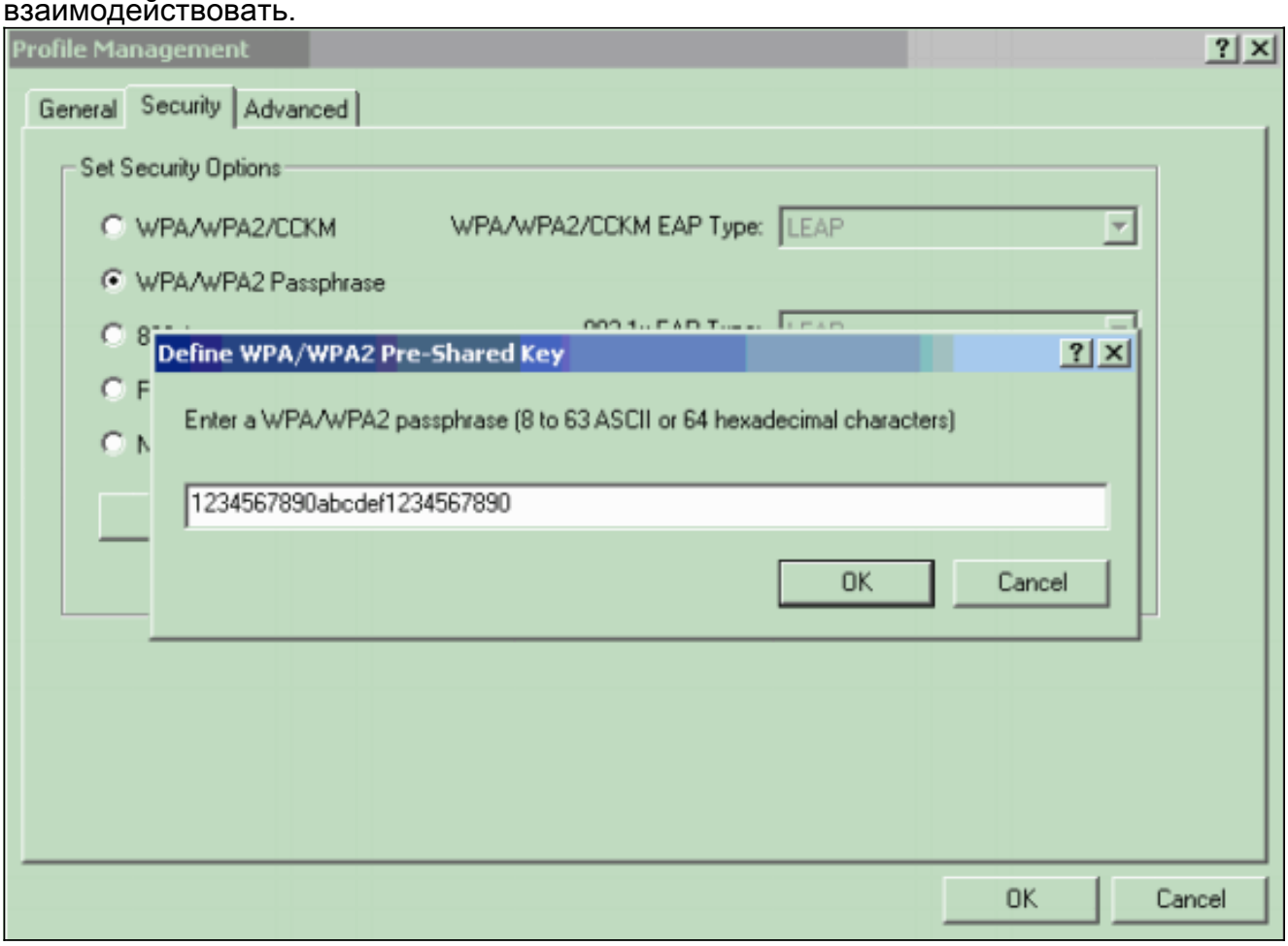
1. **В окне Profile Management на ADU необходимо нажать New, чтобы создать новый профиль.**Отобразится новое окно, в котором можно задать конфигурацию режима работы WPA 2 PSK. На закладке General ввести имя профиля (Profile Name) и SSID, который будет использоваться клиентским адаптером.В этом примере используется имя профиля WPA2-PSK и SSID – WPA2PSK:**Примечание:** SSID должен совпасть с SSID, который вы настроили на AP для WPA 2
PSK.



2. **Нажать закладку Security и нажать WPA/WPA2 Passphrase.**Это действие подключает WPA PSK или WPA 2 PSK , в зависимости от того, что было настроено на точке доступа.



3. **Нажмите кнопку Configure (Настроить).**Отобразится окно Define WPA/WPA2 Pre-Shared Key.
4. Необходимо получить у системного администратора идентификационную фразу WPA/WPA2 и ввести ее в поле WPA/WPA2 passphrase.Необходимо получить идентификационную фразу для точки доступа в инфраструктуре сети или идентификационную фразу для других клиентов в специальной сети.При введении идентификационной фразы необходимо придерживаться следующих указаний:Идентификационные фразы WPA/WPA2 должны содержать от 8 до 63 ASCII текстовых символов или 64 шестнадцатеричных символа.Идентификационная фраза клиентского адаптера должна соответствовать идентификационной фразе точки доступа, с которой планируется взаимодействовать.



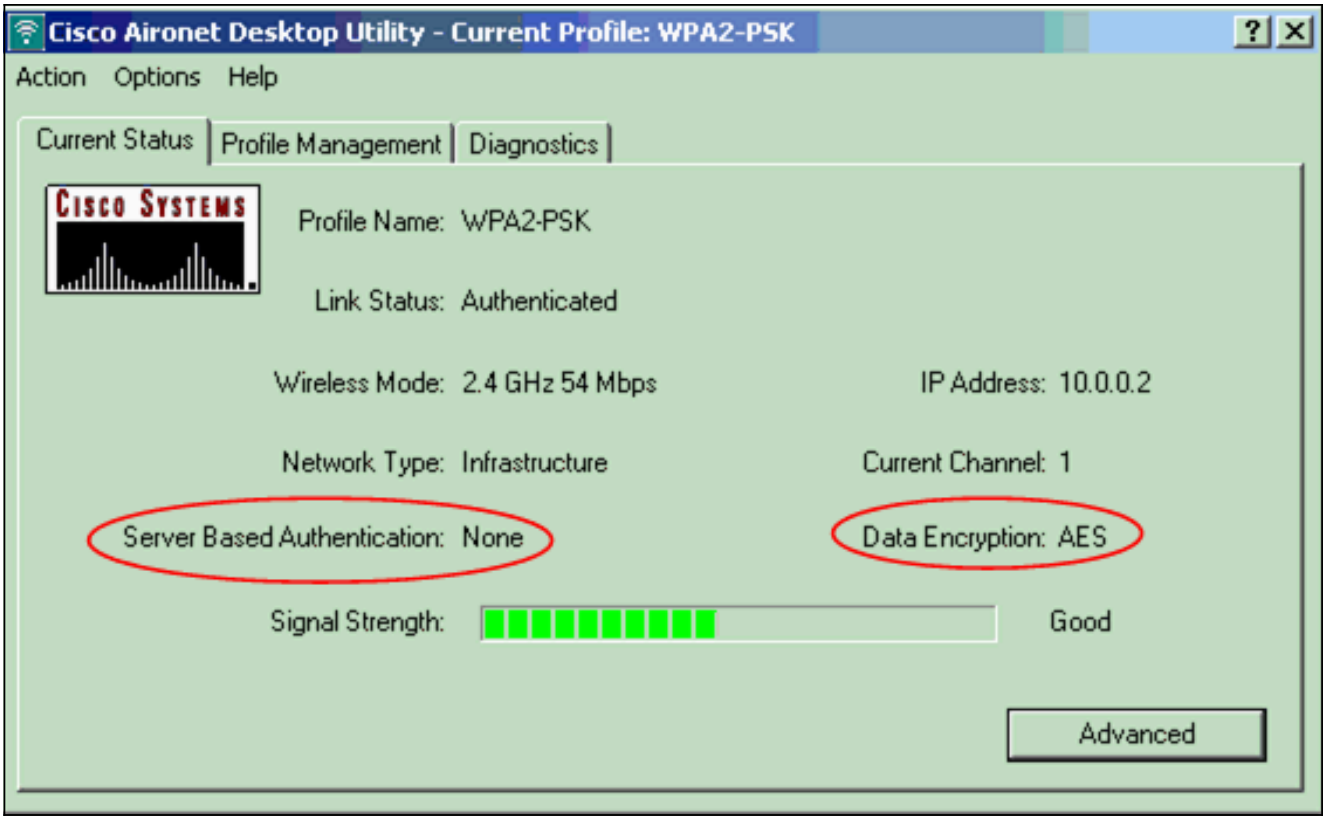
5. **Нажать OK, чтобы сохранить идентификационную фразу и вернуться в окно Profile Management.**

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

После активации профиля WPA 2 PSK точка доступа аутентифицирует клиента на основании идентификационной фразы WPA 2 (PSK) и обеспечивает доступ к WLAN.

1. Чтобы убедиться в том, что клиент успешно прошел аутентификацию, необходимо проверить ADU Current Status.Пример настройки представлен на следующем окне. В окне показано, что использовалось шифрование AES и не выполнялась серверная аутентификация:



2. Чтобы убедиться в том, что клиент успешно прошел аутентификацию при помощи режима аутентификации WPA 2 PSK , необходимо проверить журнал событий точки доступа/моста.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Настройка пакетов Cipher Suites и WEP

- Настройка типов аутентификации
- Обзор конфигурации WPA
- WPA2 - защищенный доступ по протоколу Wi-Fi 2
- То, что является WPA, смешало операцию режима, и как делают я настраиваю его в своем AP
- Страница поддержки беспроводных технологий
- Cisco Systems – техническая поддержка и документация