# Cisco Secure Services Client с проверкой подлинности EAP-FAST

## Содержание



## Введение

Этот документ описывает способ настройки клиента защищенных служб Cisco (CSSC) с контроллерами беспроводных локальных сетей, программным обеспечением Microsoft Windows® 2000 и защищенным сервером управления доступом Cisco (ACS) версии 4.0 посредством EAP-FAST. В этом документе представлена архитектура EAP-FAST с примерами развертывания и конфигурации. CSSC представляет собой компонент клиентского ПО, который обеспечивает сообщение мандатов пользователя инфраструктуре для аутентификации пользователя в сети и назначения ему соответствующих полномочий доступа.

Это некоторые преимущества решения CSSC, как выделено в этом документе:

- Аутентификация каждого пользователя (или устройство) до разрешения доступа к WLAN/LAN с Протоколом EAP
- Сквозное решение для безопасности беспроводных сетей с сервером, средством проверки подлинности и Клиентскими компонентами
- Стандартное решение для проводной и беспроводной аутентификации
- Динамичный, на пользовательские ключи шифрования произошел в процессе проверки подлинности
- Никакое требование для Инфраструктуры открытых ключей (PKI) или сертификатов (дополнительная Проверка сертификата)
- Присвоение политики доступа и/или поддерживающая NAC платформа EAP

**Примечание:** См. Проект беспроводных сетей Cisco SAFE информации о развертываниях безопасного радио.

Система аутентификации 802.1x была включена как часть 802.11i (Безопасность беспроводной локальной сети), стандарт для включения уровня 2 базировал функции аутентификации, авторизации и учета в беспроводной локальной сети 802.11. Сегодня, существует несколько протоколов EAP, доступных для развертываний и в соединенном проводом и в беспроводные сети. Обычно развертываемые протоколы EAP включают LEAP, PEAP и EAP-TLS. В дополнение к этим протоколам Cisco определила и внедрила Гибкую аутентификацию EAP через Защищенный Туннель (EAP-FAST) протокол как на основе стандартов протокол EAP, доступный для развертываний и в соединенном проводом и в беспроводные локальные сети. Спецификация протокола EAP-FAST общедоступна на веб-сайте IETF.

Как с некоторыми другими протоколами EAP, EAP-FAST является архитектурой безопасности клиент-сервер, которая шифрует транзакции EAP в туннеле TLS. В то время как подобный PEAP или EAP-TTLS в этом отношении, это отличается по той установке туннеля EAP-FAST, основано на сильных общих секретных ключах, которые уникальны для каждого пользователя по сравнению с PEAP/EAP-TTLS (которые используют сертификат X.509 сервера для защиты сеанса аутентификации). Эти общие секретные ключи называют Учетными данными Защищенного доступа (PAC) и можно распределить автоматически (Автоматическая или Внутриполосная Инициализация) или вручную (Ручная или Внеполосная Инициализация) к устройствам клиента. Поскольку квитирования, основанные на общих секретных ключах, более эффективны, чем квитирования, основанные на инфраструктуре PKI, EAP-FAST является самым быстрым и менее с высокой загрузкой процессора тип EAP тех, которые предоставляют защищенные опознавательные обмены. EAP-FAST также разработан для простоты развертываний, так как это не требует, чтобы сертификат на клиенте беспроводной локальной сети или на инфраструктуре RADIUS все же включил встроенный механизм инициализации.

Это некоторые главные возможности протокола EAP-FAST:

- Единая точка входа (SSO) с Именем пользователя в Windows / пароль
- Поддержка выполнения сценария регистрации
- Поддержка Защищенного доступа по протоколу Wi-Fi (WAP) без соискателя третьей стороны (только Windows 2000 и XP)
- Простое развертывание без требования для инфраструктуры PKI
- Устаревание Пароля Windows (т.е. поддержите для основанного на сервере истечения срока действия пароля),
- Интеграция с Cisco Trust Agent для Контроля доступа к сети с соответствующим клиентским программным обеспечением

# Предварительные условия

## Требование

Существует предположение, что установщик ознакамливается с основной установкой Windows 2003 и установкой WLC Cisco, так как этот документ только покрывает определенные конфигурации для упрощения тестов.

Для начальной установки и сведений о конфигурации для Cisco Контроллеры серии 4400, обратитесь к Краткому руководству по началу работы: Контроллеры беспроводных LAN серии Cisco 4400. Дополнительные сведения по изначальной установке и конфигурации контроллеров серии Cisco 2000 см. в Краткое руководство по началу запуска: Контроллеры беспроводных LAN серии Cisco 2000.

Перед началом установите Microsoft Windows server 2000 с последним программным обеспечением пакета обновления. Установите контроллеры и облегченные точки доступа (LAP) и гарантируйте, что настроены обновления последних версий программного обеспечения.

## Используемые компоненты

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

- Cisco 2006 или Контроллер серии 4400, который выполняется 4.0.155.5
- AP LWAPP Cisco 1242
- Windows 2000 с Active Directory
- Cisco Catalyst 3750G коммутатор
- Windows XP с картой адаптера CB21AG и версией 4.05 Cisco Secure Services Client

## Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

# Параметры дизайна

## Database

Когда вы развертываете сеть WLAN и ищете протокол аутентификации, это обычно желаемо для использования текущей базы данных для пользователя/аутентификации компьютера. Типичные базы данных, которые могут использоваться, являются Windows Active Directory, LDAP или базой данных Одноразового пароля (OTP) (т.е. RSA или SecureID). Все эти базы данных совместимы с протоколом EAP-FAST, но когда вы планируете развертывания, существуют некоторые Требования совместимости, которые нужно рассмотреть. Первоначальное развертывание файла PAC клиентам выполнено посредством анонимной автоинициализации, аутентифицировал инициализацию (через сертификат X.509 текущего клиента) или ручную инициализацию. В целях этого документа рассматривают анонимную автоинициализацию и ручную инициализацию.

Автоматическая инициализация PAC использует Аутентифицируемый Протокол соглашения о Ключе Диффи-Хеллмана (ADHP) для установления безопасного туннеля. Безопасный туннель может быть установлен или анонимно или через механизм проверки подлинности сервера. В соединении установки туннеля MSCHAPv2 используется, чтобы аутентифицировать клиента и, после успешной аутентификации, распределить файл PAC клиенту. После того, как PAC был успешно настроен, файл PAC может использоваться для инициирования нового сеанса аутентификации EAP-FAST для получения доступа защищенной сети.

Автоматическая инициализация PAC относится к базе данных в использовании, потому что, так как механизм автоинициализации полагается на MSCHAPv2, база данных, используемая для аутентификации пользователей, должна быть совместима с этим форматом пароля. При использовании EAP-FAST с базой данных, которая не поддерживает формат MSCHAPv2 (такой как OTP, Novell, или LDAP), это требуется, чтобы использовать некоторый другой механизм (т.е. инициализация руководства или аутентифицируемая инициализация) для развертывания пользовательских файлов PAC. Этот документ дает пример автоматической инициализации с базой данных Пользователя Windows.

## Шифрование

Аутентификация EAP-FAST не требует использования определенный тип шифрования WLAN. Тип шифрования WLAN, который будет использоваться, определен клиентскими возможностями платы NIC. Рекомендуется использовать WPA2 (CCM AES) или WPA (TKIP) шифрование, зависящее от возможностей платы NIC в определенных развертываниях. Обратите внимание на то, что решение для WLAN Cisco позволяет сосуществование и WPA2 и устройств клиента WPA на общем SSID.

Если устройства клиента не поддерживают WPA2 или WPA, возможно развернуть аутентификацию 802.1X с динамическими Ключами WEP, но, из-за известного использования против Ключей WEP, этот механизм шифрования WLAN не рекомендуется. Если это требуется, чтобы поддерживать клиентов только для WEP, рекомендуется использовать интервал session-timeout, который требует, чтобы клиенты получили новый Ключ WEP на частом интервале. Тридцать минут являются рекомендуемым интервалом сеанса для типичных скоростей передачи данных WLAN.

## Единая точка входа и учетные данные машины

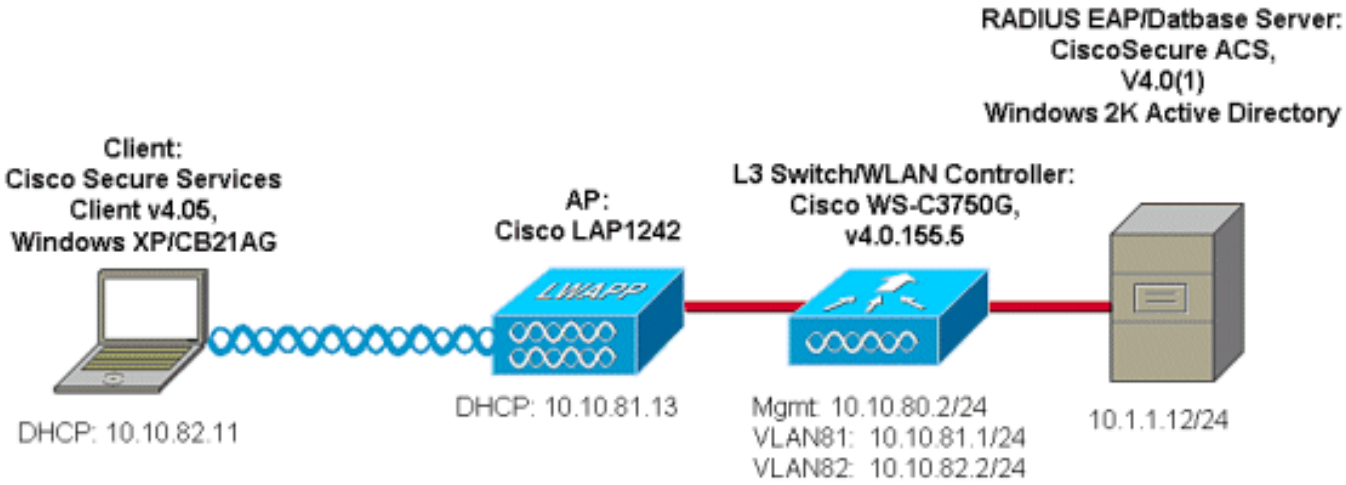
Единая точка входа обращается к способности входа в систему одиночного пользователя или записи учетных данных для аутентификации, которые будут использоваться для доступа к составным приложениям или составным устройствам. В целях этого документа Единая точка входа обращается к использованию учетных данных, которые используются для входа ПК для аутентификации к WLAN.

С Cisco Secure Services Client возможно использовать учетные данные начала сеанса пользователя, чтобы также аутентифицироваться на сети WLAN. Если это желаемо для аутентификации, ПК к сети до пользователя входят в систему к ПК, это требуется, чтобы использовать или сохраненные учетные данные пользователя или учетные данные, связанные к профилю машины. Или этих методов полезно в случаях, где это желаемо, чтобы выполнить сценарии входа в систему или подключить диски, когда ПК загружается, в противоположность когда входы пользователя в систему на.

# Схема сети

Это - Схема сети, используемая в этом документе. В этой сети существует четыре используемые подсети. Обратите внимание на то, что необязательно для сегментации этих устройств в другие сети но это предоставляет наибольшую гибкость для интеграции с реальными сетями. Catalyst 3750G Интегрированный Контроллер беспроводной локальной сети предоставляет Питание над Ethernet (POE) switchports, коммутацию L3 и возможность Контроллера беспроводной локальной сети на обычной проблеме, связанной с шасси.

1. Сеть 10.1.1.0 является сетью сервера, где находится ACS.
2. Сеть 10.10.80.0 является сетью управления, используемой Контроллером беспроводной локальной сети.
3. Сеть 10.10.81.0 является сетью, где находятся AP.
4. Сеть 10.10.82.0 используется для клиентов WLAN.




# Настройте Access Control Server (ACS)

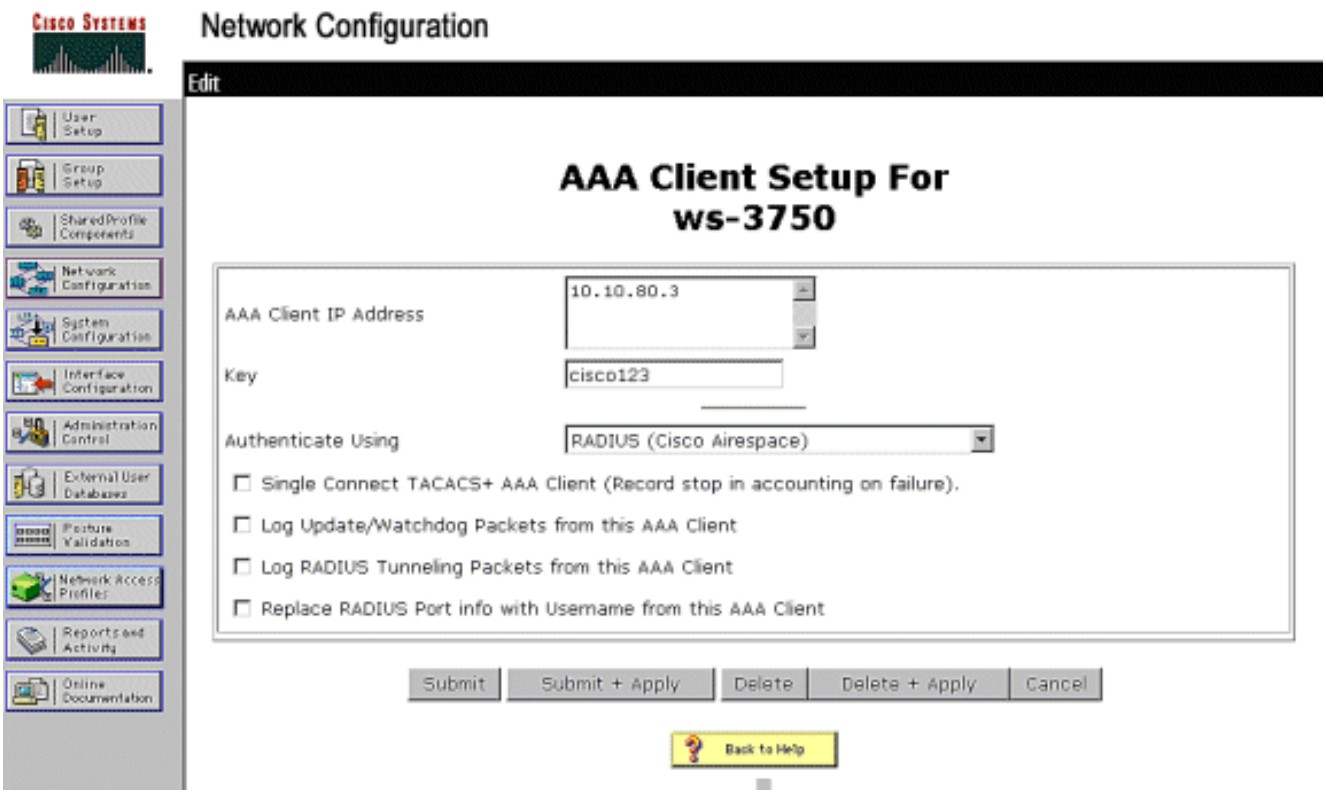
В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

**Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

## Добавьте точку доступа как клиента AAA (NAS) в ACS

В этом разделе описывается настроить ACS для EAP-FAST с внутриполосной инициализацией PAC с Windows Active Directory как внешняя база данных.

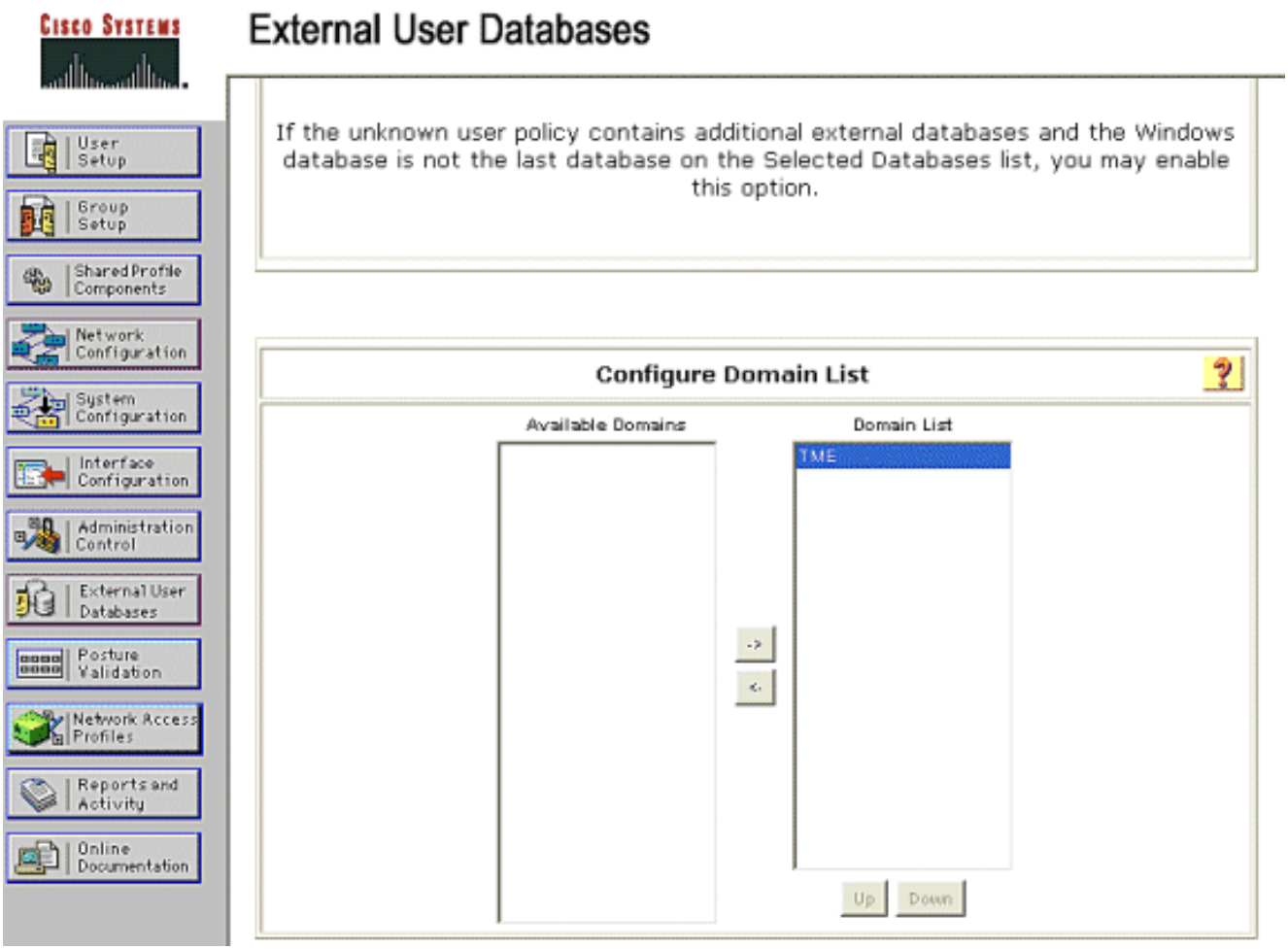
1. **Необходимо зарегистрироваться в ACS > Network Configuration и щелкнуть Add Entry.**
2. Заполните название Контроллера беспроводной локальной сети, IP-адрес, общий секретный ключ, и под Используемой аутентификацией, выберите RADIUS (Cisco Airespace), который также включает атрибуты IETF RADIUS.**Примечание:** Если Группы сетевых устройств (NDG) включены, сначала выбирают соответствующий NDG и добавляют Контроллер беспроводной локальной сети к нему. См. Руководство Конфигурации AcS для подробных данных о NDG.
3. **Нажмите Submit +**
   **Restart.**



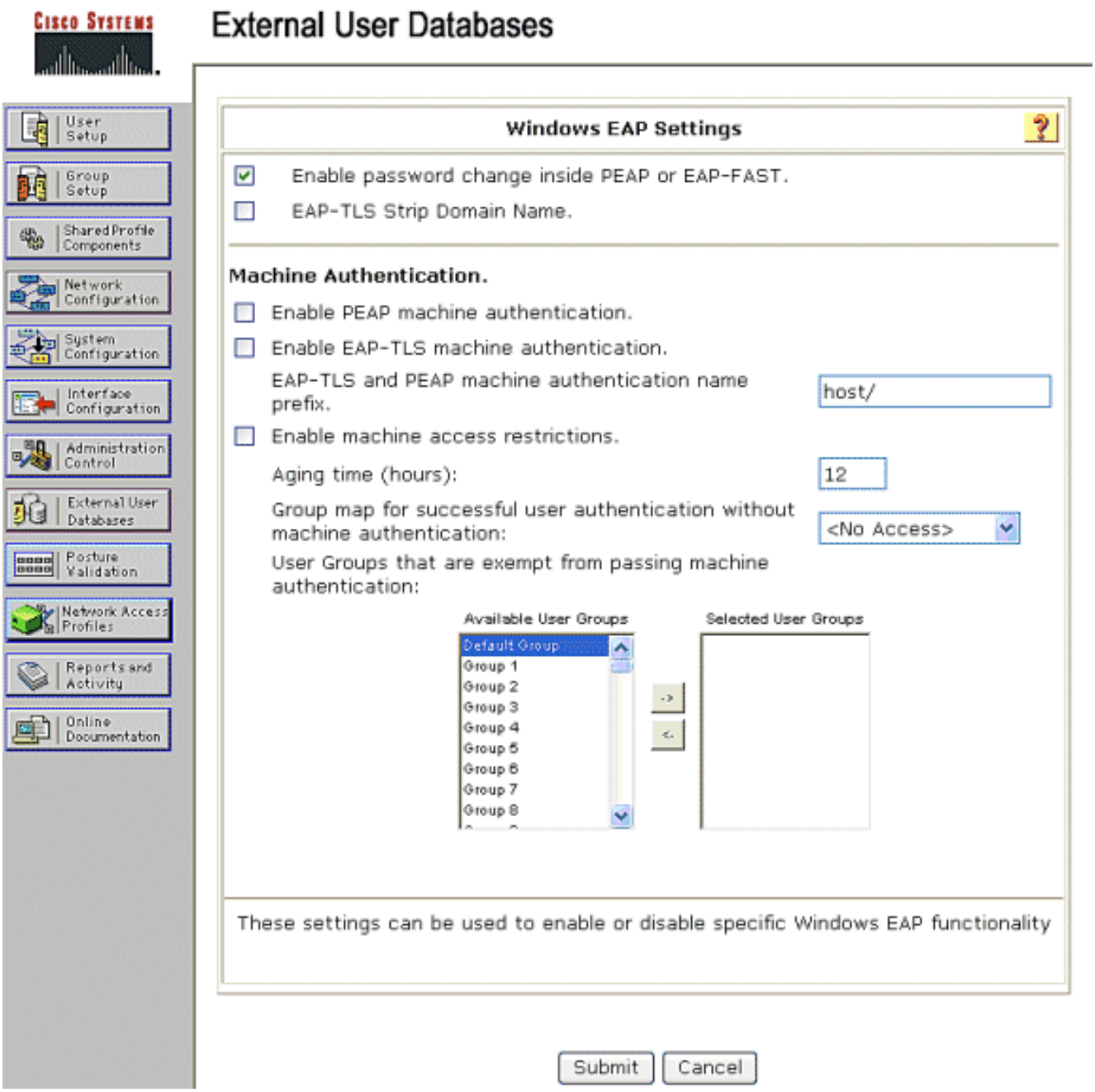

## Настройте ACS для запроса внешней базы данных

В этом разделе описывается настроить ACS для запроса внешней базы данных.

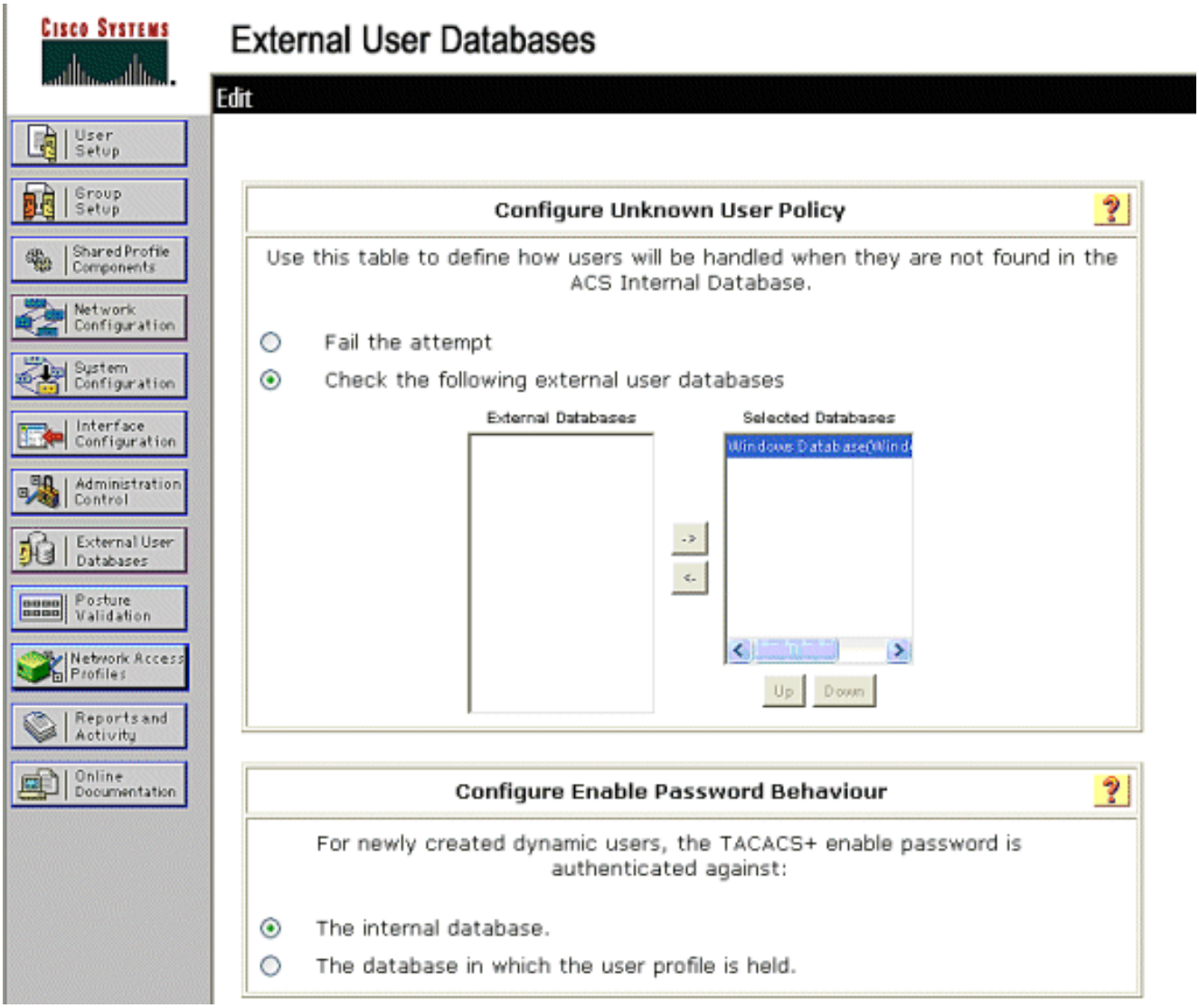
1. **Нажмите External User Database > Database Configuration > Windows Database > Configure.**
2. **В поле "Configure Domain List" переместите Domains из списка "Available Domains" в список "Domain".Примечание:** Сервер, который выполняет ACS, должен ознакомиться с этими доменами для приложения ACS, чтобы обнаружить и использовать те цели доменов для проверки
подлинности.




3. Под Windows EAP Settings настройте опцию для разрешения изменения пароля в сеансе EAP-FAST или PEAP. См. Руководство по конфигурации для Cisco Secure ACS 4.1 для получения большего количества подробных данных об устаревании Пароля Windows и EAP-FAST.
4. **Нажмите кнопку Submit (Отправить).Примечание:** Можно также активировать опцию Разрешения набора номера для EAP-FAST под Конфигурацией базы данных Пользователя Windows, чтобы разрешить внешней базе данных Windows управлять разрешением доступа. Параметры настройки MS-CHAP для изменения пароля на странице конфигурации Базы данных Windows только применимы к аутентификации MS-CHAP не-EAP. Чтобы к enable password изменяются в сочетании с EAP-FAST, это необходимо для изменения enable password под Windows EAP Settings.




5. **Нажмите External User Database > Unknown User Policy и выберите Check the following external user databases.**
6. **Переместите базу данных Windows из окна External Databases в окно Selected Databases.**
7. **Нажмите кнопку Submit (Отправить).Примечание:** С этого момента ACS проверяет Windows DB. Если пользователь не найден в локальной базе данных ACS, она размещает пользователя в группу по умолчанию ACS. См. документацию ACS для получения дополнительной информации о Сопоставлениях групп баз данных.**Примечание:** Поскольку ACS делает запрос базы данных Microsoft Active Directory для проверки учетных данных пользователя, дополнительные параметры настройки прав доступа должны быть настроены на Windows. См. [Руководство по установке для Cisco Secure ACS для Windows Server] для подробных данных.



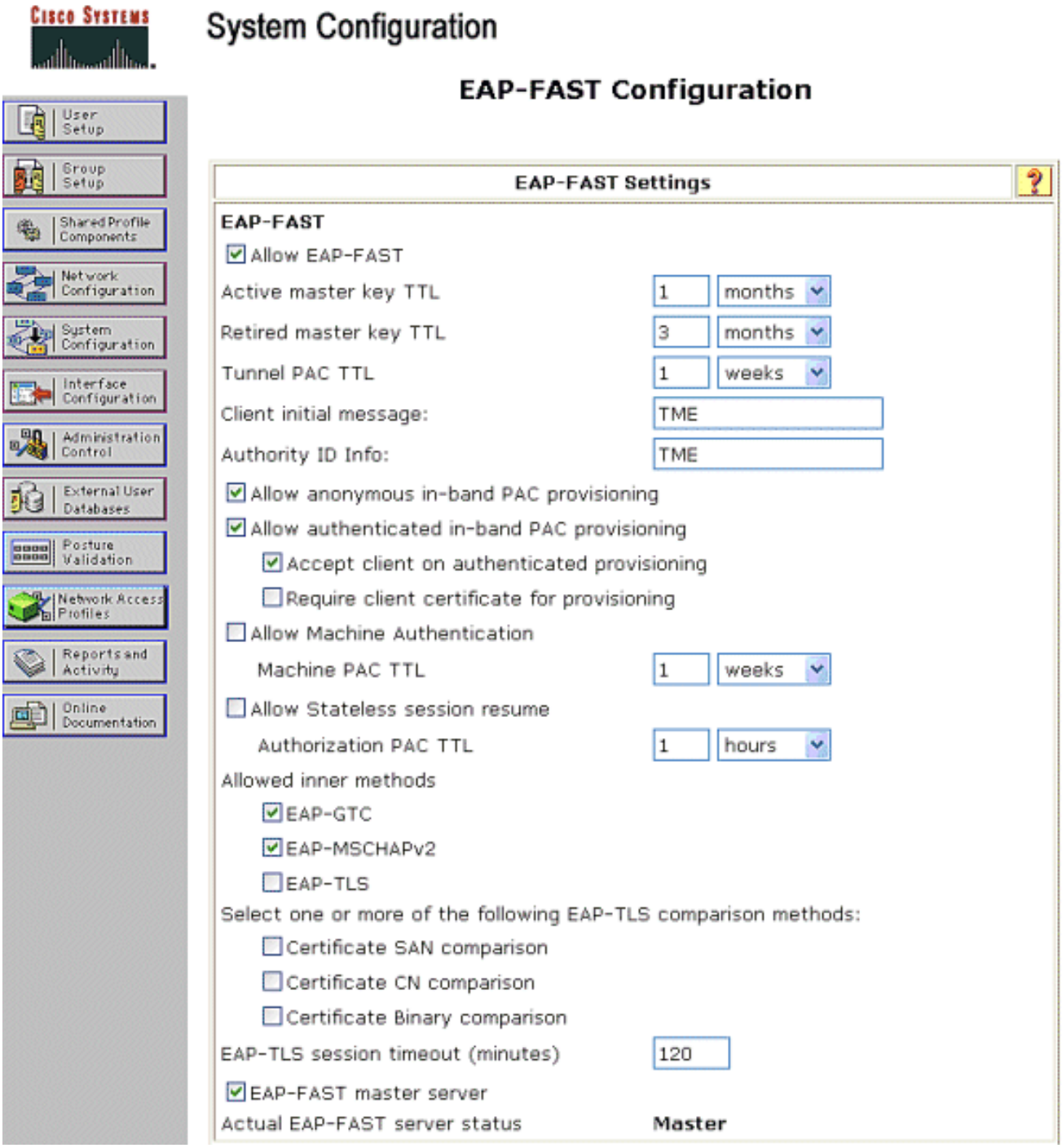

## Включите поддержку EAP-FAST на ACS

В этом разделе описывается включить поддержку EAP-FAST на ACS.

1. **Перейдите в System Configuration > Global Authentication Setup > EAP-FAST Configuration.**
2. **Выберите Allow EAP-FAST.**
3. Настройте эти рекомендации: TTL Главного ключа / Исключенный TTL главного ключа / TTL PAC. Эти параметры настройки настроены по умолчанию в Cisco Secure ACS:Главный ключ месяц TTL:1Исключенный Ключевой TTL: 3 месяцаTTL PAC: 1 неделя
4. **Заполните поле Authority ID Info.** Этот текст показывают на некотором клиентском программном обеспечении EAP-FAST, где выбор полномочий PAC является контроллером.**Примечание:** Cisco Secure Services Client не использует этот описательный текст для полномочий PAC.
5. **Выберите поле Allow in-band PAC provisioning.** Это поле включает Автоматическую Инициализацию PAC для должным образом поддерживающих клиентов EAP-FAST. Для данного примера используется автоинициализация.
6. **Выберите Allowed inner methods:** EAP-GTC и MSCHAP2 EAP. Это разрешает использование и v1 EAP-FAST и клиентов EAP-FAST v1a. (Cisco Secure Services Client поддерживает EAP-FAST v1a.), Если необязательно поддержать клиентов v1 EAP-

FAST, только необходимо включить EAP-MSCHAPv2 как внутренний метод.

7. **Установите флажок EAP-FAST Master Server для активизации данного сервера EAP-FAST в качестве основного.** Это разрешает другим серверам ACS использовать этот сервер как основные полномочия PAC для предотвращения условия уникальных ключей для каждого ACS в сети. См. Руководство Конфигурации AcS для подробных данных.
8. **Нажмите Submit + Restart.**




## Контроллер беспроводной локальной сети Cisco

В целях этого Руководства по развертыванию Cisco WS3750G Интегрированный Контроллер беспроводной локальной сети (WLC) используется с AP Легкого веса Cisco AP1240 (LAP) для обеспечения инфраструктуры WLAN для тестов CSSC. Конфигурация применима для любого контроллера беспроводной локальной сети Cisco. Используемая

версия программного обеспечения 4.0.155.5.

# Настройте контроллер беспроводной локальной сети

## Главная операция и регистрация LAP к контроллеру

Используйте мастер запуска конфигурации в интерфейсе командной строки (CLI) для настройки WLC в основном режиме. Также можно использовать GUI для настройки WLC. В данном документе описана конфигурация на WLC, выполняемая с помощью мастера запуска конфигурации в CLI.

После того, как WLC загружается впервые, он вводит в мастера загрузочной конфигурации. Используйте мастера настройки для настройки базовых параметров. Можно обратиться к мастеру через CLI или GUI. Эти выходные данные отображают пример мастера запуска конфигурации в CLI:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: ws-3750 Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): ***** Management Interface IP Address:
10.10.80.3 Management Interface Netmask: 255.255.255.0 Management Interface Default Router:
10.10.80.2 Management Interface VLAN Identifier (0 = untagged): Management Interface DHCP Server
IP Address: 10.10.80.2 AP Manager Interface IP Address: 10.10.80.4 AP-Manager is on Management
subnet, using same values AP Manager Interface DHCP Server (172.16.1.1): Virtual Gateway IP
Address: 1.1.1.1 Mobility/RF Group Name: Security Network Name (SSID): Enterprise Allow Static
IP Addresses [YES][no]: yes Configure a RADIUS Server now? [YES][no]: no Warning! The default
WLAN security policy requires a RADIUS server. Please see documentation for more details. Enter
Country Code (enter 'help' for a list of countries) [US]: Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes Enable 802.11g Network [YES][no]: yes Enable Auto-RF
[YES][no]: yes Configuration saved! Resetting system with new configuration.
```

Данные параметры используются, чтобы настроить WLC для выполнения основных операций. **В данном примере конфигурации в WLC используется 10.10.80.3 в качестве IP-адреса интерфейса управления и 10.10.80.4 в качестве IP-адреса интерфейса AP-диспетчера.**

Прежде чем любые другие функции могут быть настроены на WLC, LAP должны зарегистрироваться в WLC. Этот документ предполагает, что LAP зарегистрирован к WLC. См. Регистр Легковесный AP к разделу WLC Аварийного переключения Контроллера беспроводной локальной сети для Примера конфигурации Облегченных точек доступа для получения информации о том, как Легковесные AP регистрируются в WLC. Для ссылки с этим примером конфигурации AP1240s развернуты на отдельной подсети (10.10.81.0/24) от контроллера беспроводной локальной сети (10.10.80.0/24), и параметр DHCP 43 используется для обеспечения обнаружения контроллера.

## Проверка подлинности RADIUS через Cisco Secure ACS

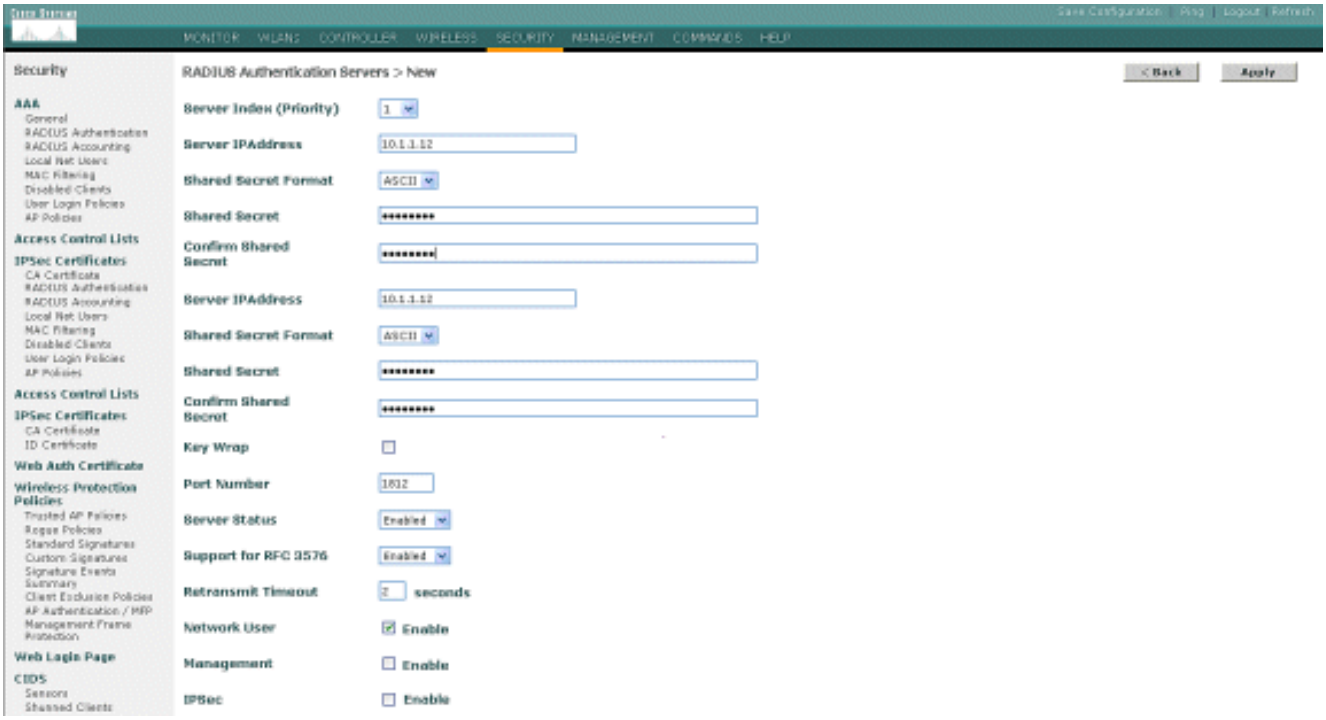
WLC должен быть настроен для передачи учетных данных пользователя серверу Cisco Secure ACS. Сервер ACS тогда проверяет учетные данные пользователя (через настроенную Базу данных Windows) и предоставляет доступ к беспроводным клиентам.

Выполните эти шаги для настройки WLC для связи к серверу ACS:

1. **Нажмите Security и RADIUS Authentication в контроллере GUI, чтобы открыть страницу**

"RADIUS Authentication Servers". Чтобы задать сервер RADIUS, необходимо нажмите New.


2. Определите параметры сервера ACS на странице RADIUS Authentication Servers> New. Эти параметры включают IP-адрес ACS, Общий секретный ключ, Номер порта и Состояние сервера.**Примечание:** Номера портов 1645 или 1812 совместимы с ACS для Проверки подлинности RADIUS.Флажки Network User и Management определяют, просит ли основанная на RADIUS аутентификация пользователей сети (например, клиенты WLAN) и управление (т.е. административные пользователи). Пример конфигурации использует Cisco Secure ACS в качестве сервера RADIUS с IP-адресом 10.1.1.12:



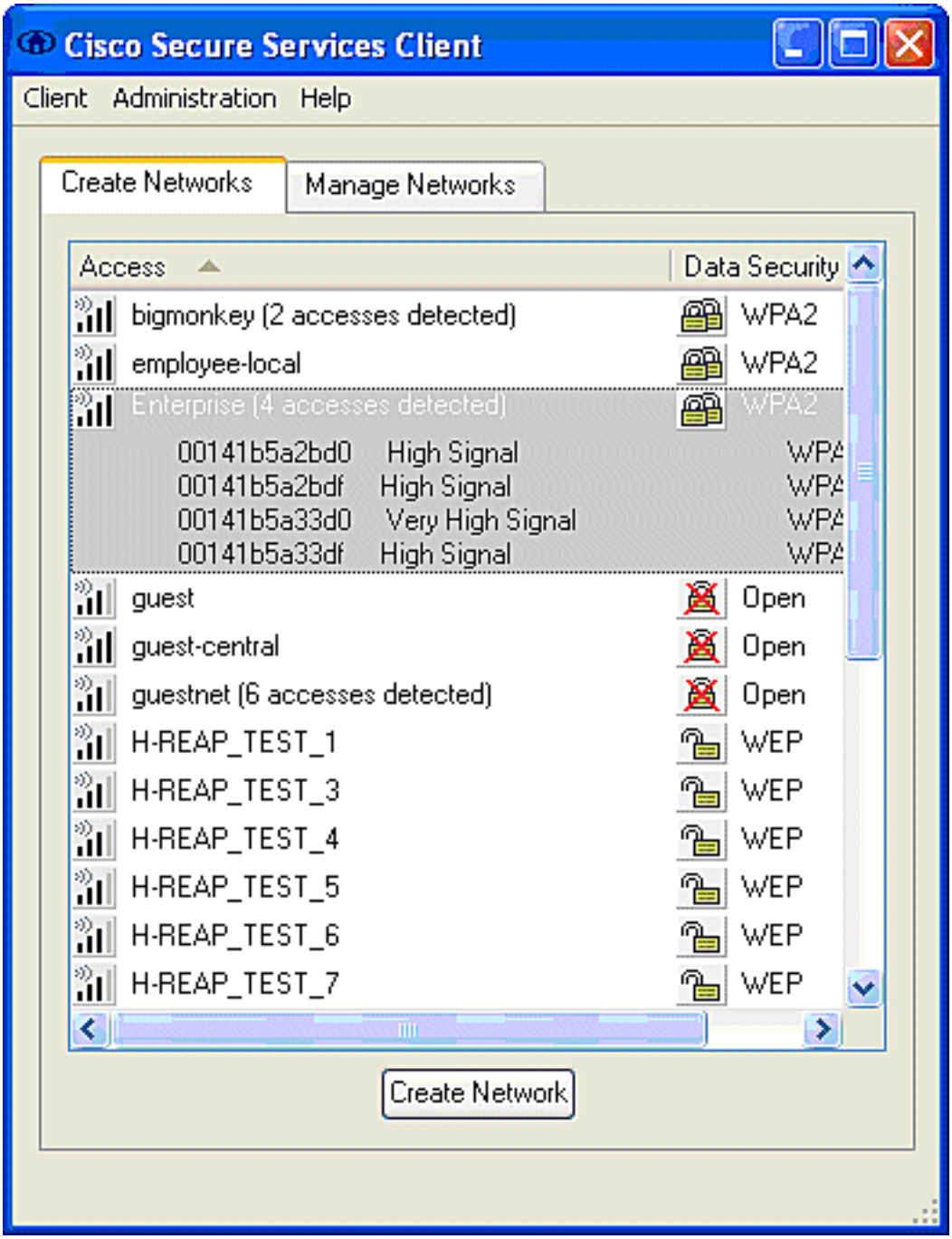

## Конфигурация параметров WLAN

В этом разделе описываются конфигурацию Cisco Secure Services Client. В данном примере CSSC v4.0.5.4783 используется с клиентским адаптером Cisco CB21AG. До установки программного обеспечения CSSC проверьте, что только драйверы для CB21AG установлены, не служебная программа рабочего стола Aironet (ADU).

Как только программное обеспечение установлено, и оно выполняется как сервис, оно просматривает для доступных сетей и отображает доступных.

**Примечание:** CSSC отключает Windows Zero Config.

**Примечание:** Только те SSID, которые включены для широковещания, видимы.




**Примечание:** Контроллер беспроводной локальной сети, по умолчанию, передает SSID, таким образом, это показывают в Создать Списке сетей просмотренного SSIDs. **Чтобы создать профиль сети, в списке нажмите SSID (Enterprise), затем кнопку Create Network.**

**Если инфраструктура WLAN настроена на передачу отключенных SSID, необходимо вручную добавить SSID. В устройствах доступа нажмите кнопку Add, вручную введите подходящий SSID (например, Enterprise). Настройте активное состояние образца для клиента, т.е., где клиент активно проводит испытание для своей настроенной SSID. Укажите Actively search for this access device, после того, как будет введен SSID в окне Add Access Device.**

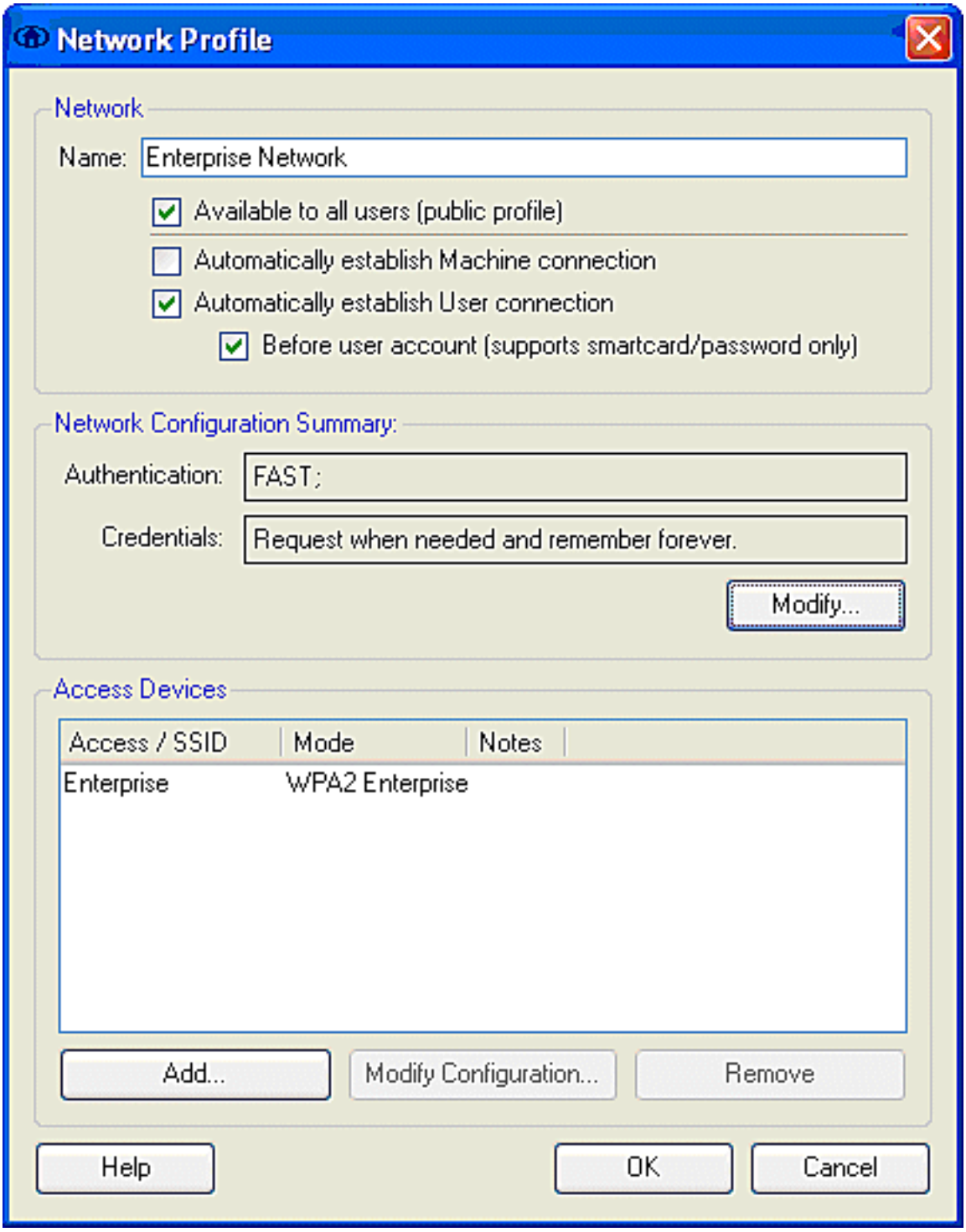
**Примечание:** Если параметры настройки Аутентификации eap сначала не настроены для профиля, параметры порта не разрешают расширенные режимы (802.1X).

**Кнопка Create Network запускает окно Network Profile, которое позволяет связываться с выбранными (или настроенными) SSID с аутентификационным механизмом.** Назначьте описательное имя для профиля.

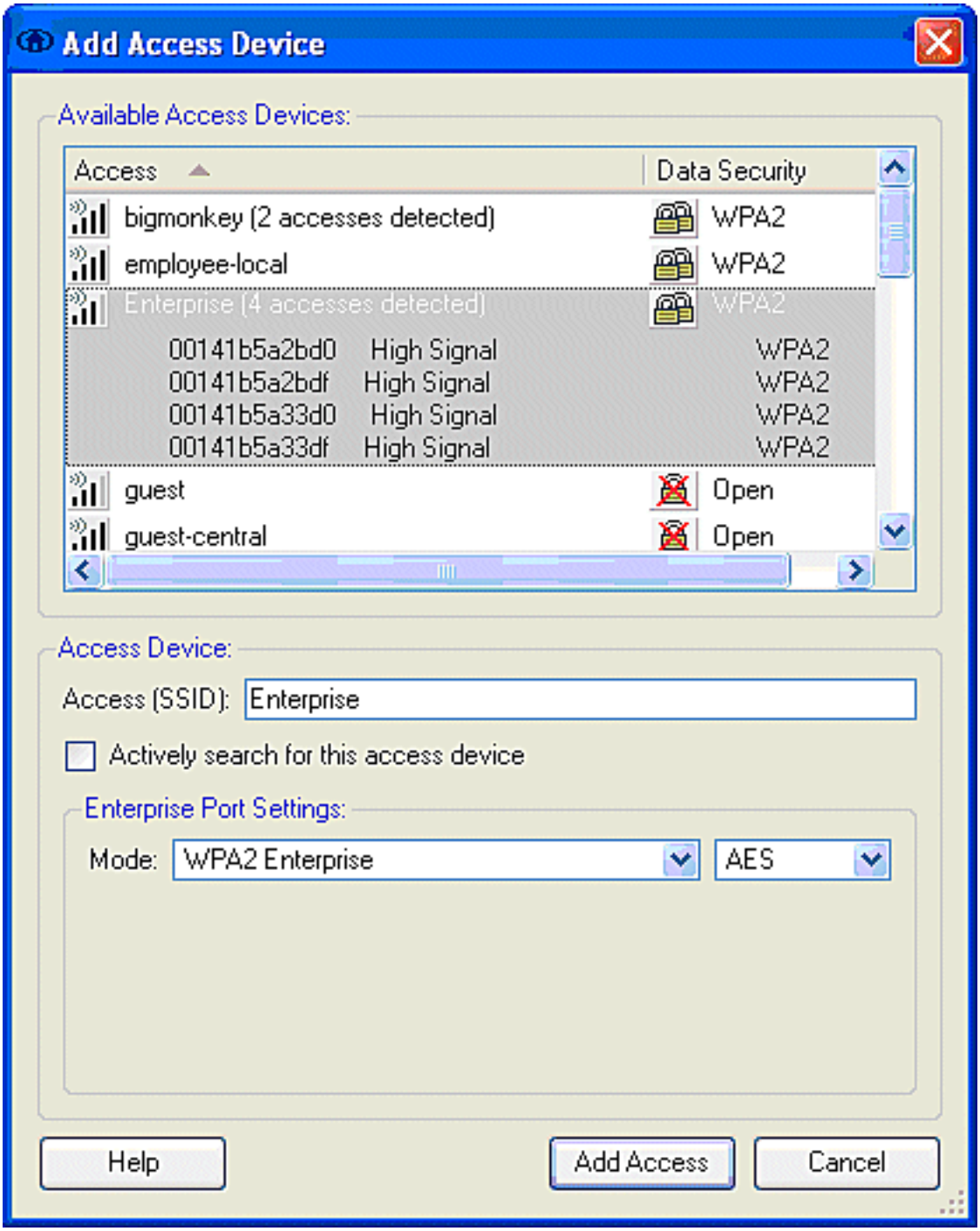
**Примечание:** Множественные типы безопасности беспроводных сетей и/или SSIDs могут быть привязаны под этим опознавательным профилем.

**Чтобы клиент автоматически соединялся с сетью при нахождении в зоне действия радиосвязи, выберите Automatically establish User connection. Снимите флажок с Available to all users, если использование данного профиля для других учетных записей пользователей на данном устройстве нежелательно. Если Automatically establish не выбрано, необходимо, чтобы пользователь открыл окно CSSC и вручную запустил WLAN подключение кнопкой Connect.**

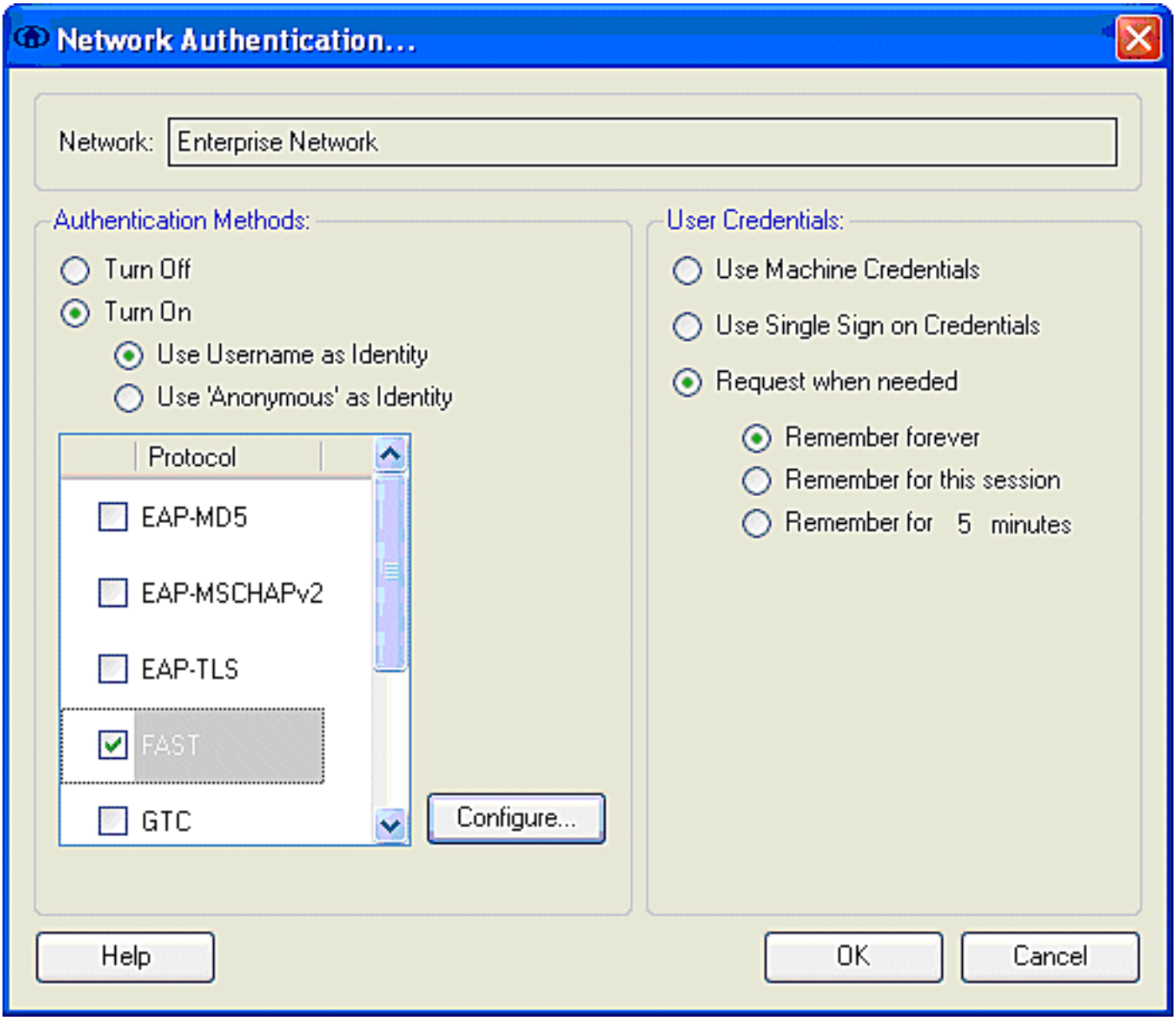
**Если требуется запустить WLAN- подключение до входа в систему пользователем, выберите Before user account.** Это разрешает операцию Единой точки входа с учетными данными сохраненного пользователя (пароль или сертификат/Смарт-карта при использовании TLS в EAP-FAST).



**Примечание:** Для операции WPA/TKIP с Клиентским адаптером Cisco Aironet серии 350 необходимо отключить проверку квитирования WPA, так как в настоящее время существует несовместимость между клиентом CSSC и 350 драйверами относительно проверки хэша квитирования WPA. **Эта проверка отключается в Client > Advanced Settings > WPA/WPA2 Handshake Validation.** Отключенная проверка квитирования все еще разрешает характеристики безопасности, свойственные от WPA (TKIP попакетное манипулирование и Message Integrity Check), но отключает начальную аутентификацию ключа WPA.




**В "Network Configuration Summary" нажмите Modify, чтобы настроить параметры EAP/учетных данных. Нажмите Turn On, чтобы включить аутентификацию. Выберите в FAST в "Protocol", затем выберите 'Anonymous' as Identity (чтобы не использовать имя пользователя в начальном запросе EAP). Возможно использование Use Username as Identity в качестве внешней идентификации EAP, но многие клиенты не желают открывать идентификаторы пользователя в начальном незашифрованном запросе EAP. Укажите Use Single Sign on Credentials, чтобы использовать журнал учетных данных для аутентификации сети. Нажмите Configure, чтобы настроить параметры EAP-FAST.**




**В настройках FAST возможно указать Validate Server Certificate, что позволяет клиенту проверять сертификат сервера EAP-FAST (ACS) до установления сеанса EAP-FAST.** Это обеспечивает защиту для устройств клиента с соединения на неизвестный или посторонний сервер EAP-FAST и непреднамеренного подчиненного их учетных данных для аутентификации к недоверяемому источнику. Это действительно требует, чтобы серверу ACS установили сертификат, и у клиента также есть соответствующий установленный сертификат Корневого центра сертификации. В данном примере не включена проверка серверного сертификата.

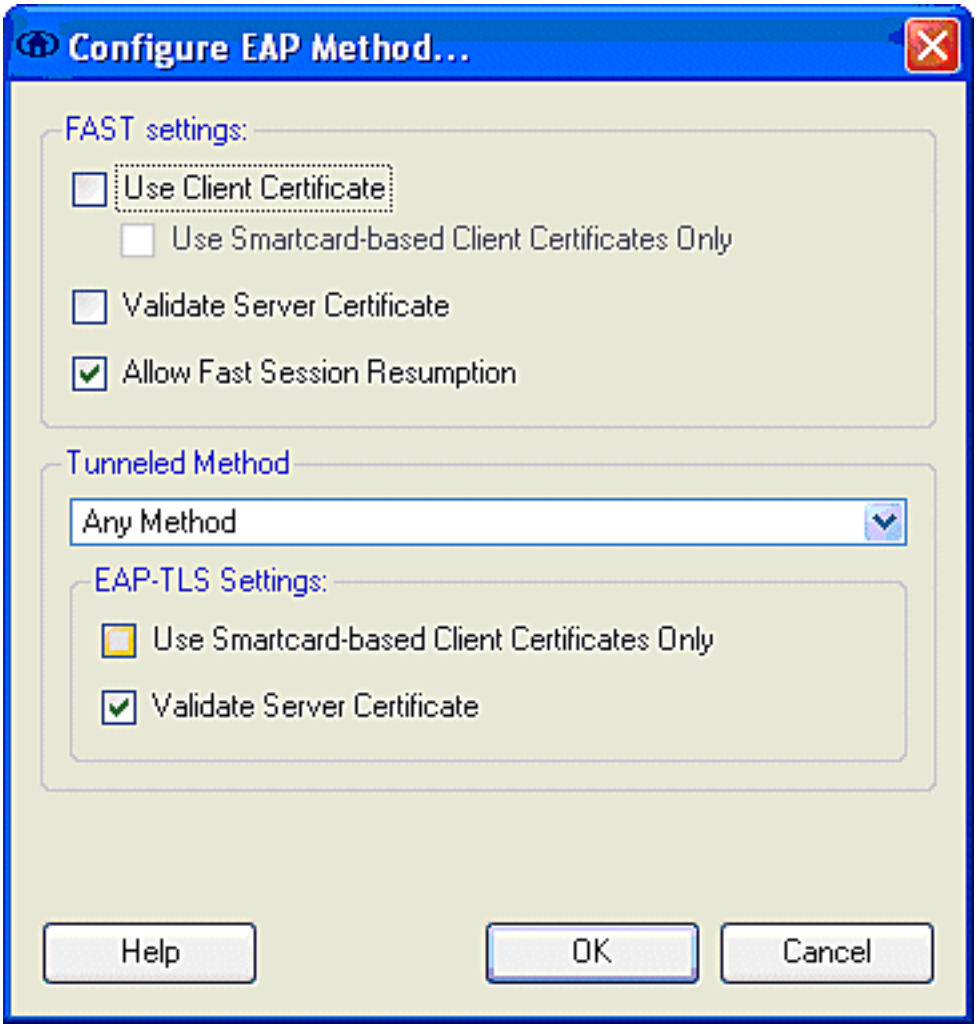
**В настройках FAST возможно указать Allow Fast Session Resumption, что разрешает возобновление сеанса EAP-FAST на основе информации о туннеле (сеанса TLS), а не на основе требования полной повторной аутентификации EAP-FAST.** Если у сервера EAP-FAST и клиента есть общепринятая истина информации о сеанса TLS, о которой выполняют согласование в рамках начального обмена аутентификации EAP-FAST, возобновление сеанса может произойти.

**Примечание:** И сервер EAP-FAST и клиент должны быть настроены для резюме сеанса EAP-FAST.

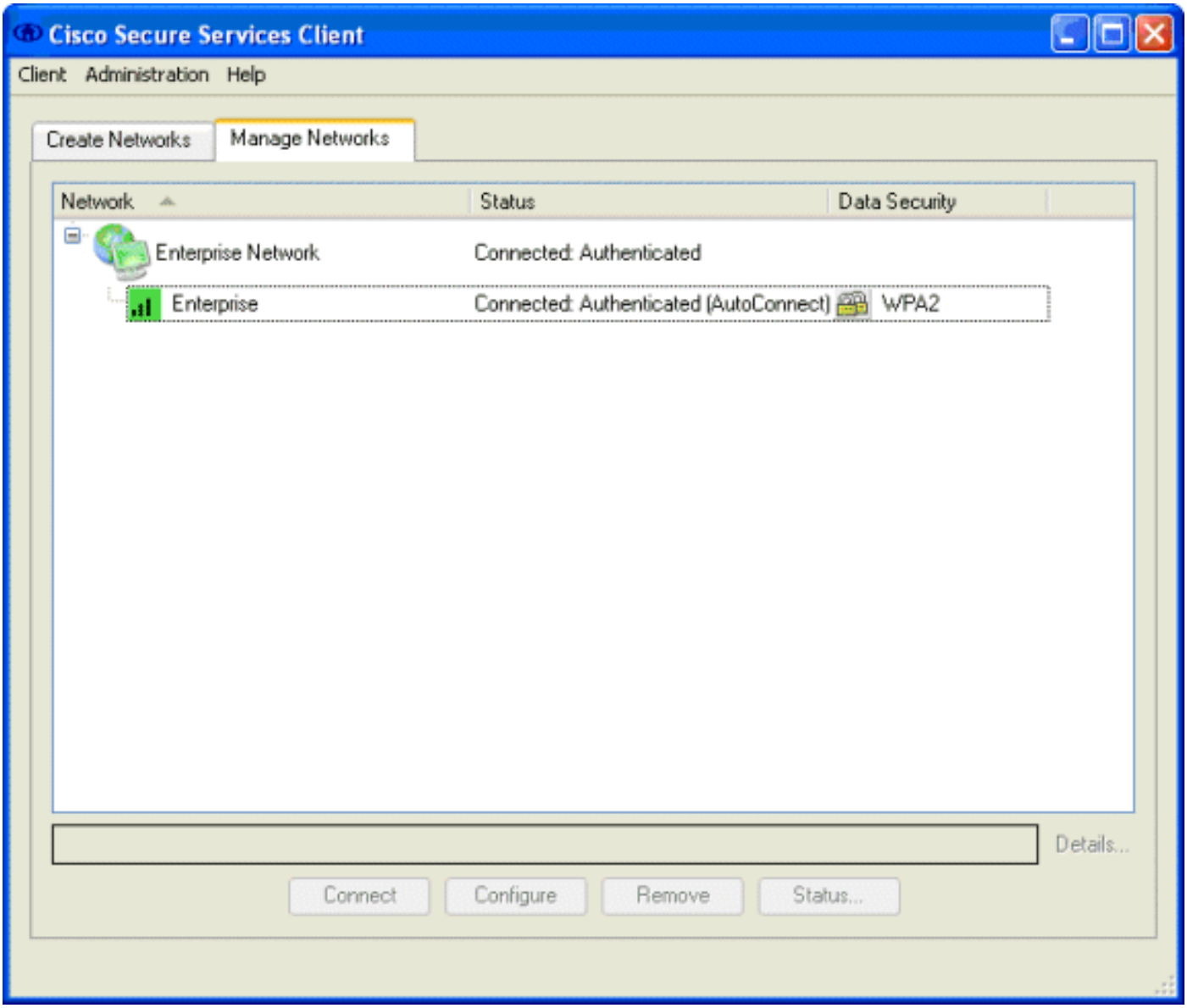
**В Tunneled Method > EAP-TLS Settings, укажите Any Method, чтобы разрешить EAP-MSCHAPv2 для автоматической настройки PAC и EAP-GTC для аутентификации. Если**

**используется база данных формата Microsoft, например, Active Directory, и если она не поддерживает клиентов EAP-FAST v1 в сети, можно также указать использование одного MSCHAPv2 в качестве метода туннелирования.**

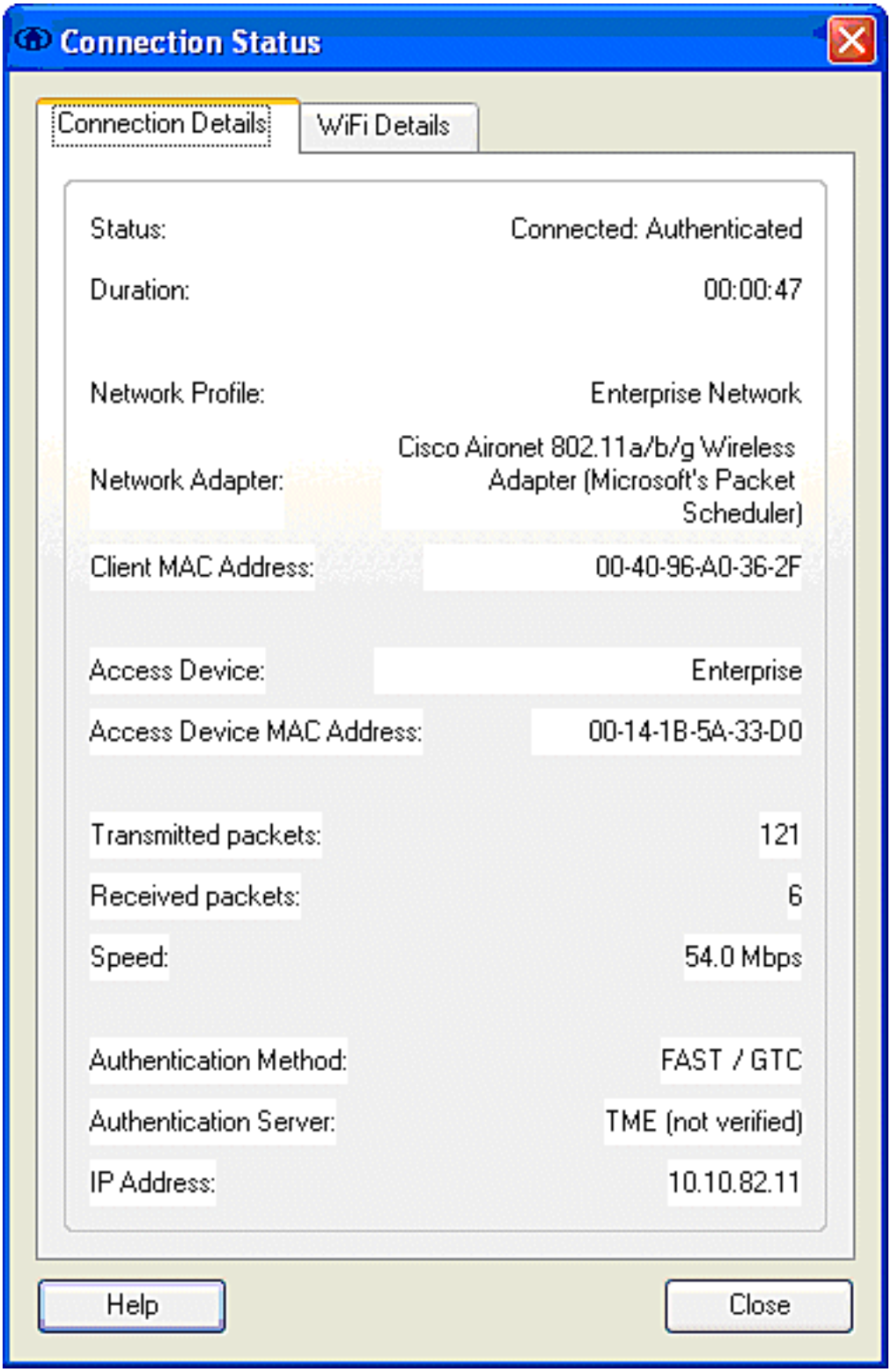
**Примечание:** Проверьте Серверный сертификат, включен по умолчанию при параметрах настройки EAP-TLS на этом окне. Так как пример не использует EAP-TLS в качестве внутреннего метода аутентификации, это поле не применимо. Если это поле включено, оно позволяет клиенту проверить серверный сертификат в дополнение к проверке сервера сертификата клиента в EAP-TLS.

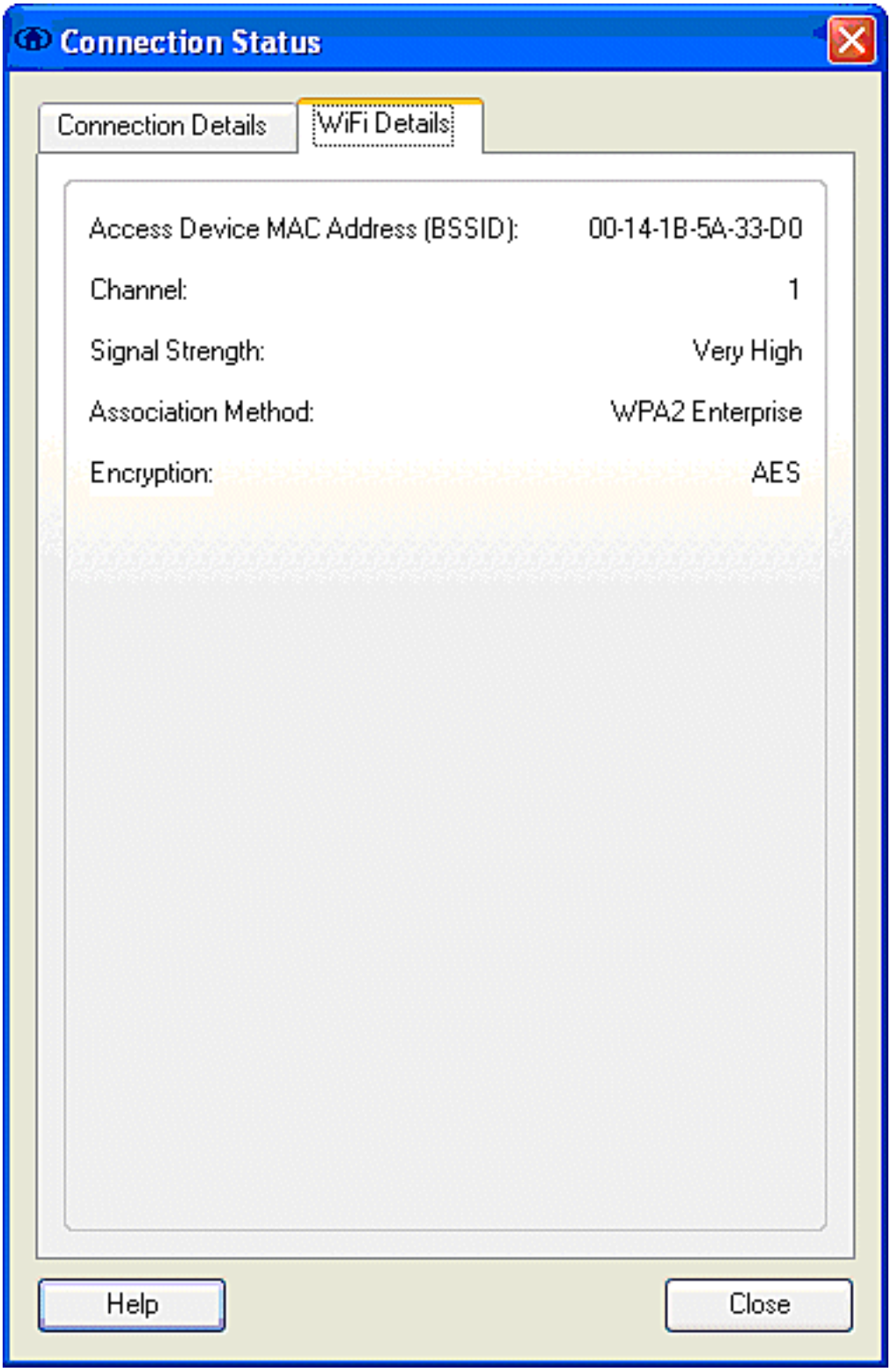



**Нажмите OK, чтобы сохранить настройки EAP-FAST.** Так как клиент настроен для, "автоматически устанавливают" под профилем, он автоматически инициирует ассоциацию/аутентификацию с сетью. От вкладки Manage Networks Сеть, Статус и поля Data Security указывают на статус соединения клиента. От примера замечено, что Корпоративная сеть Профиля используется, и Устройством Доступа к сети является Предприятие SSID, которое указывает на Connected:Authenticated и использует Autoconnect. Поле Data Security указывает на тип шифрования 802.11, который используется, который, для данного примера, является WPA2.




**После аутентификации клиента, выберите SSID в профиле во вкладке управления сетями и нажмите Status, чтобы выполнить запрос по сведениям подключения.** Окно Connection Details предоставляет сведения об устройстве клиента, статусе соединения и статистике и методе аутентификации. Вкладка WiFi Details предоставляет подробную информацию о статусе соединения 802.11, который включает RSSI, канал 802.11 и аутентификацию/шифрование.


Connection Status
Connection Details
WiFi Details
Status:
Connected: Authenticated
Duration:
00:00:47
Network Profile:
Enterprise Network
Network Adapter:
Cisco Aironet 802.11a/b/g Wireless Adapter (Microsoft's Packet Scheduler)
Client MAC Address:
00-40-96-A0-36-2F
Access Device:
Enterprise
Access Device MAC Address:
00-14-1B-5A-33-D0
Transmitted packets:
121
Received packets:
6
Speed:
54.0 Mbps
Authentication Method:
FAST / GTC
Authentication Server:
TME (not verified)
IP Address:
10.10.82.11
Help
Close




Как системный администратор, вы названы на диагностическую утилиту, Системный Отчёт о Cisco Secure Services Client, который доступен со стандартным распределением CSSC. Эта утилита доступна от меню Пуск или из каталога CSSC. **Чтобы получить данные, нажмите Collect Data > Copy to Clipboard > Locate Report File**. Это направляет Microsoft File Explorer window к каталогу с заархивированным файлом отчета. В заархивированном файле большинство полезных данных расположено под журналом (log_current).

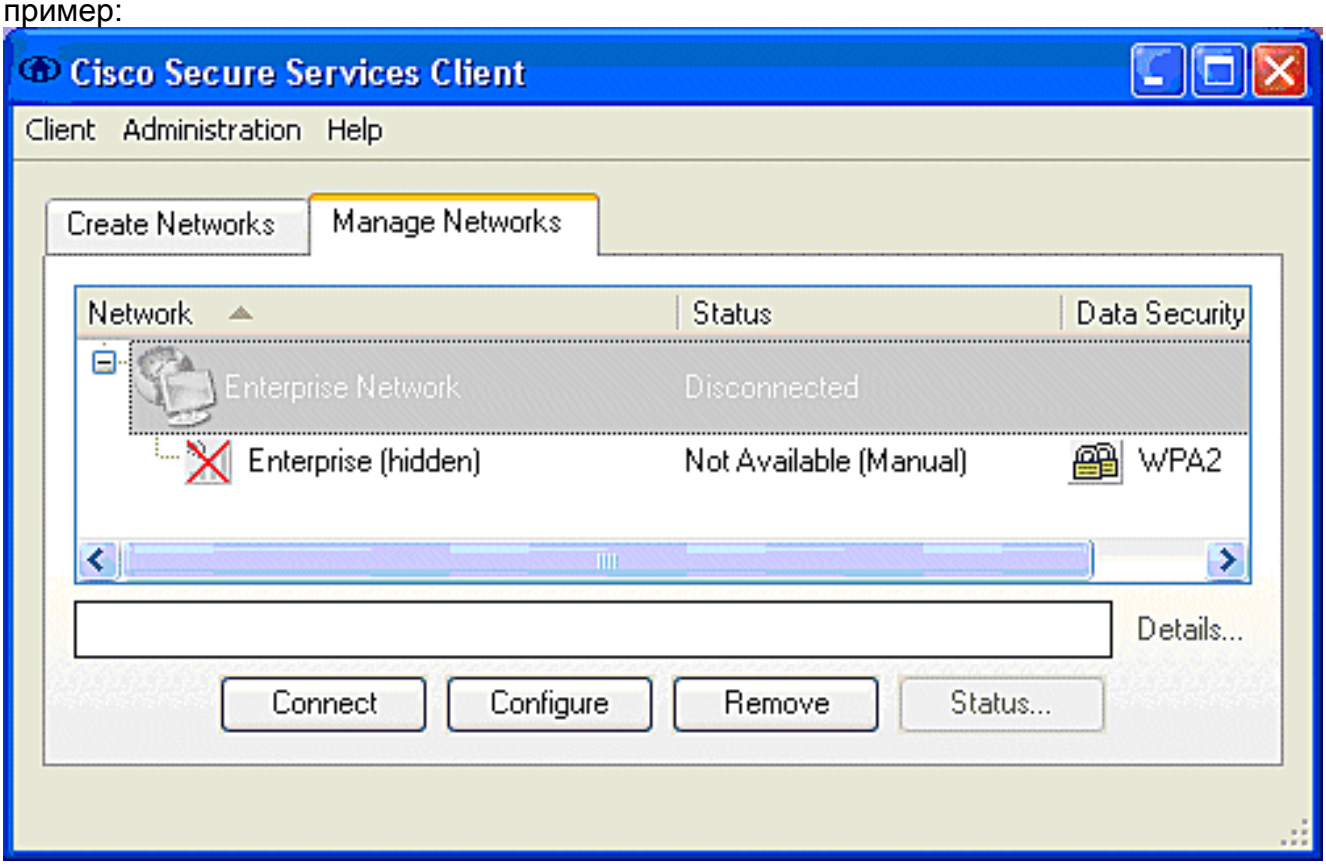
Утилита дает текущий статус CSSC, интерфейса и подробных данных драйвера, наряду с информацией о WLAN (обнаруженный SSID, статус сопоставления, и т.д.). Это может быть полезно, особенно для диагностирования проблем с подключением между CSSC и адаптером WLAN.

# Проверьте операцию

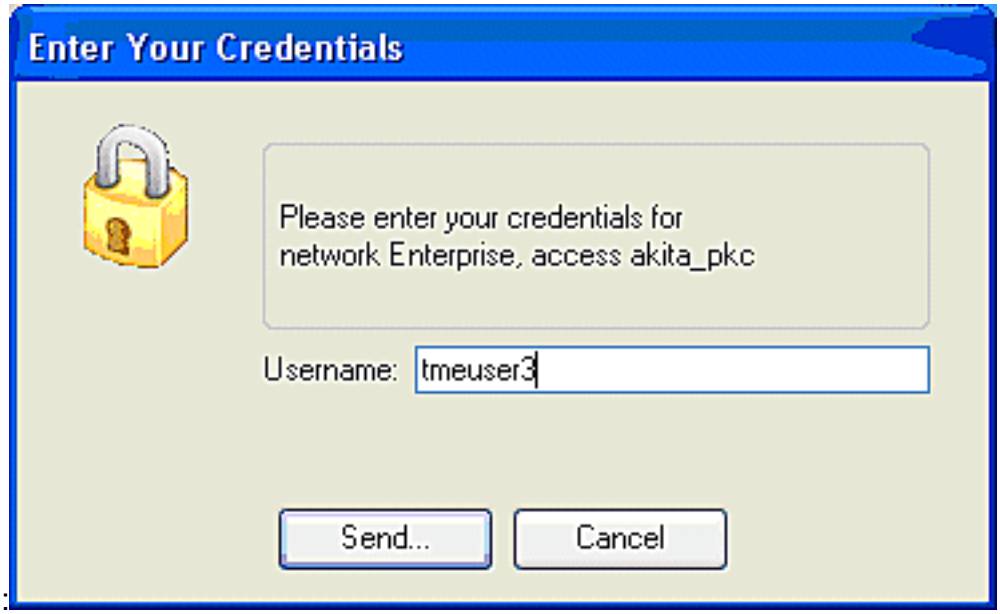
После конфигурации сервера Cisco Secure ACS, контроллера беспроводной локальной сети, клиента CSSC, и по-видимому корректной конфигурации и населения базы данных, сеть WLAN настроена для аутентификации EAP-FAST и безопасной связи с клиентом. Существуют многочисленные точки, которые могут быть проверены для проверки выполнения / ошибки для безопасного сеанса.

Для тестирования конфигурации попытайтесь привязать беспроводного клиента к Контроллеру беспроводной локальной сети с аутентификацией EAP-FAST.

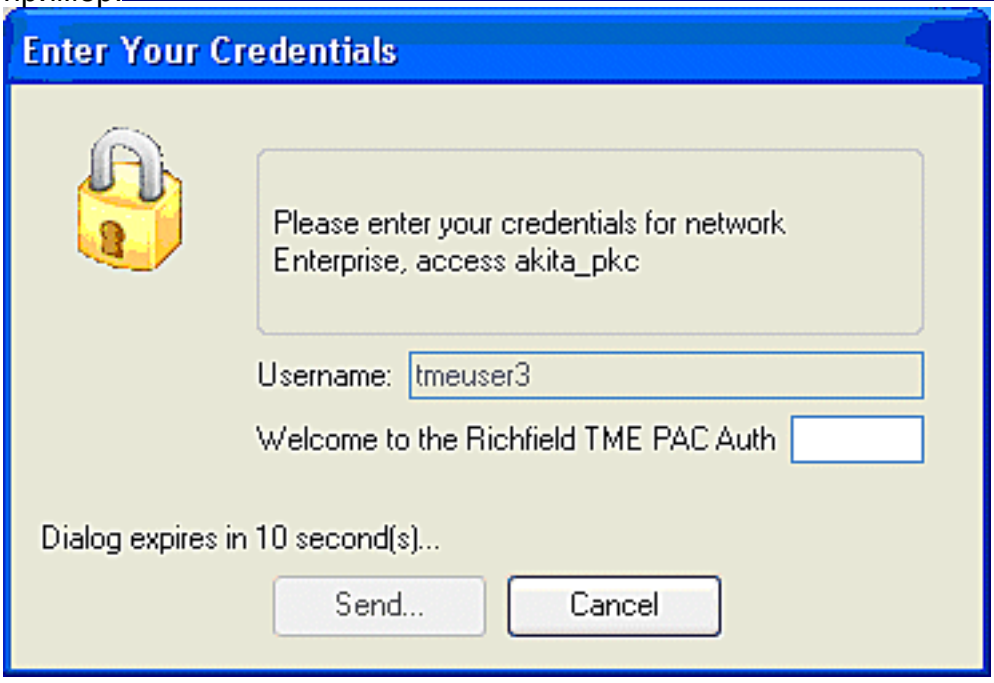
1. Если CSSC настроен для Автосоединения, клиент делает попытку этого соединения автоматически. **Если он не настроен на автоматическое соединение и функцию однократного предъявления пароля, пользователю необходимо инициировать подключение WLAN с помощью кнопки Connect**. Это инициирует процесс сопоставления 802.11, по которому происходит Аутентификация eap.Ниже представлен пример:



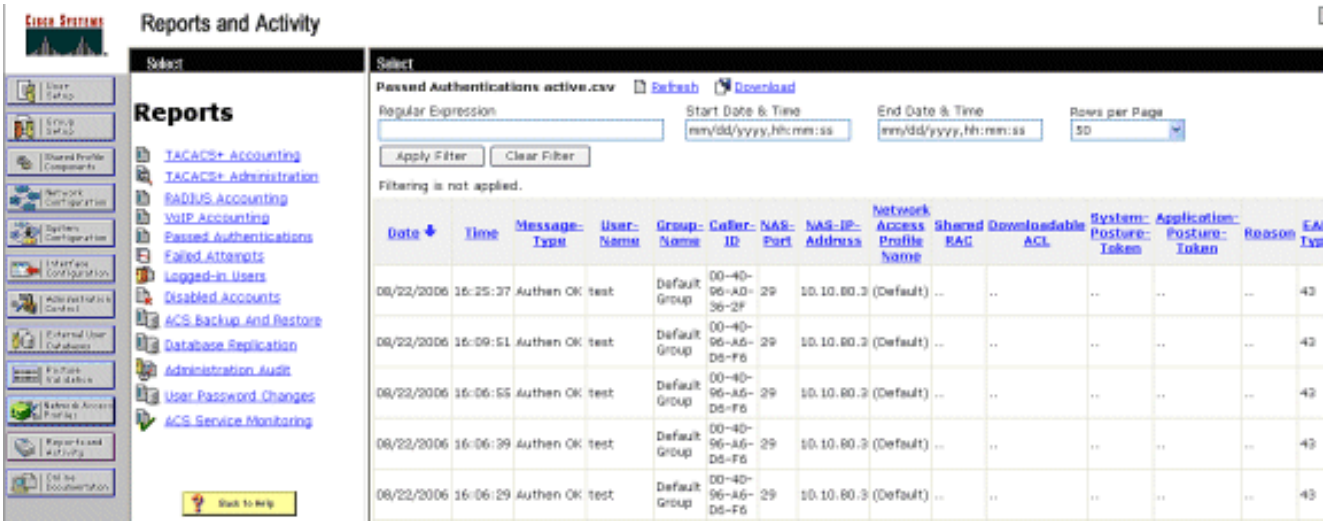

2. Пользователю впоследствии предлагают ввести имя пользователя и затем пароль для аутентификации EAP-FAST (от полномочий PAC EAP-FAST или ACS).Ниже представлен



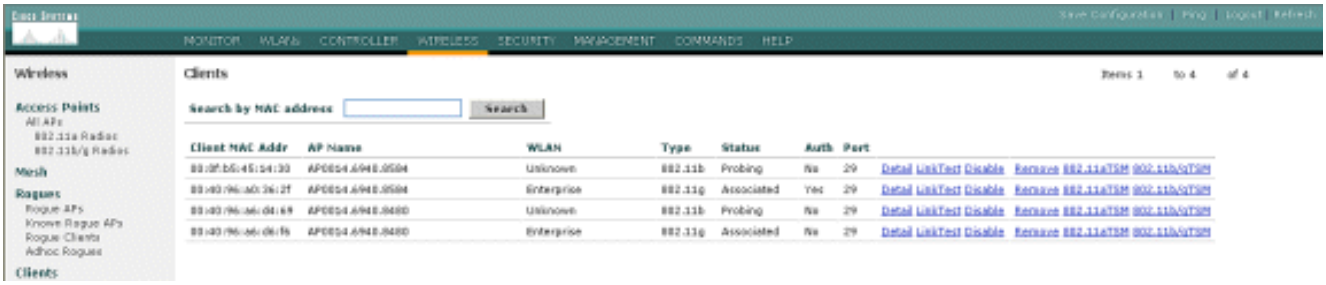

пример:




3. Клиент CSSC, посредством WLC, затем передает учетные данные пользователя к серверу RADIUS (Cisco Secure ACS) для проверки учетных данных. ACS проверяет учетные данные пользователя со сравнением данных и настроенной базы данных (в примере конфигурации, внешняя база данных является Windows Active Directory), и предоставляет доступ к беспроводному клиенту каждый раз, когда учетные данные пользователя допустимы. Переданный отчёт об Аутентификациях относительно сервера ACS показывает, что клиент передал RADIUS/АУТЕНТИФИКАЦИЮ EAP.Ниже представлен
пример:




4. На успешный RADIUS/АУТЕНТИФИКАЦИЮ EAP беспроводной клиент (00:40:96:ab:36:2f в данном примере) аутентифицируется с AP / контроллер беспроводной локальной
сети.




## Приложение

В дополнение к диагностике и сведениям о статусе, которые доступны в Cisco Secure ACS и контроллере беспроводной локальной сети Cisco, существуют дополнительные точки, которые могут использоваться для диагностирования аутентификации EAP-FAST. Несмотря на то, что большинство проблем аутентификации может быть диагностировано без использования анализатора WLAN или обменов EAP отладки в контроллере беспроводной локальной сети, этот справочный материал включен, чтобы помочь устранять неполадки.

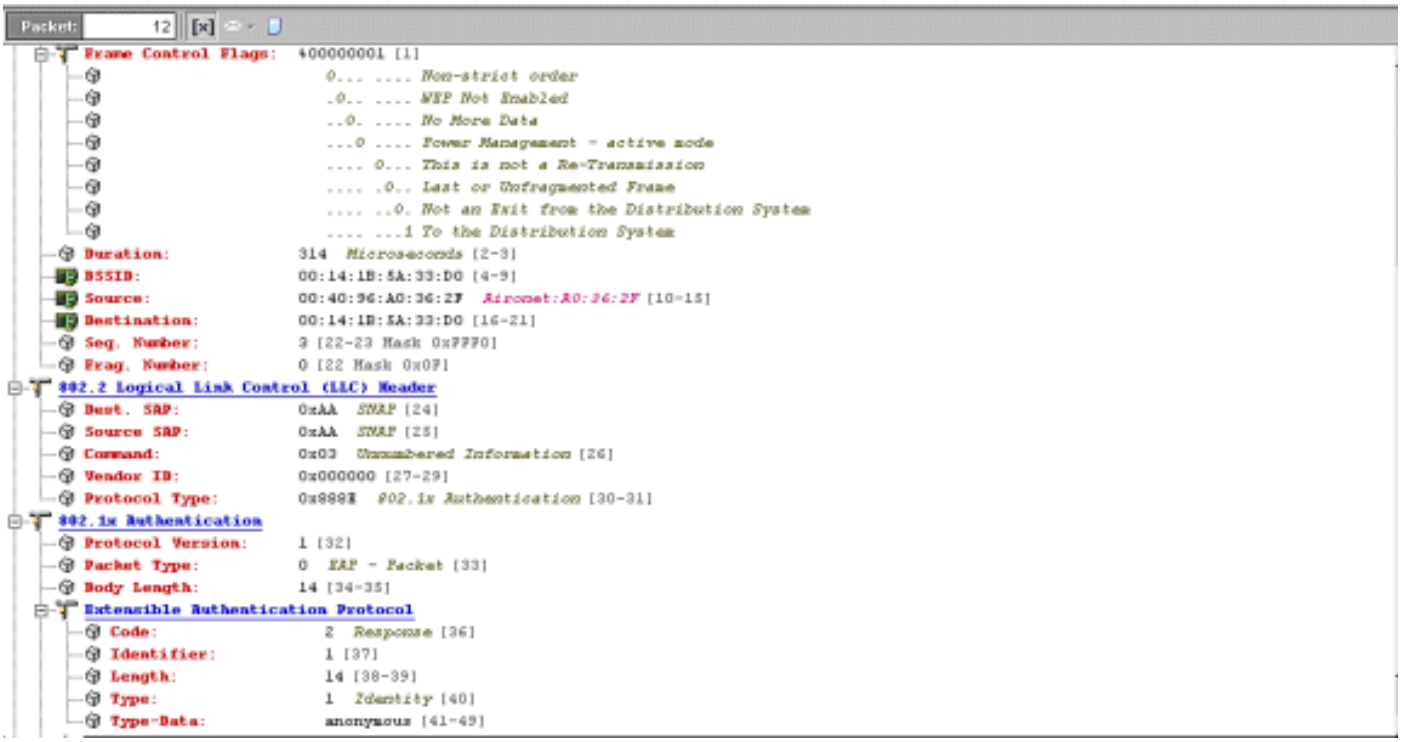
### Перехват анализатора для Exchange EAP-FAST

Этот перехват анализатора 802.11 показывает опознавательный обмен.

| Source | Flags | Channel | Signal | Data Rate | Size | Relative Time | Protocol | Summary |
|---|---|---|---|---|---|---|---|---|
| 00:14:1B:5A:33:D0 | * | 11 | 68% | 36.0 | 101 | 00.033877 | 802.11 Assoc Rsp | FC=...R....,SN=2867,FN= 0,Status... |
| 00:14:1B:5A:33:D0 | * | 11 | 70% | 24.0 | 101 | 00.036453 | 802.11 Assoc Rsp | FC=...R....,SN=2867,FN= 0,Status... |
| 00:14:1B:5A:33:D0 | | 11 | 71% | 54.0 | 90 | 00.036494 | 802.1x | FC=.F......,SN=2868,FN= 0 |
| Aironet:A0:36:2F | | 11 | 54% | 1.0 | 82 | 00.123205 | EAP Response | FC=T.......,SN= 3,FN= 0 |
| 00:14:1B:5A:33:D0 | # | 11 | 71% | 1.0 | 14 | 00.123517 | 802.11 Ack | FC=........ |
| 00:14:1B:5A:33:D0 | | 11 | 67% | 54.0 | 65 | 00.165611 | 802.1x | FC=.F......,SN=2870,FN= 0 |
| Aironet:A0:36:2F | | 11 | 55% | 1.0 | 82 | 00.173920 | EAP Response | FC=T.......,SN= 4,FN= 0 |
| 00:14:1B:5A:33:D0 | # | 11 | 70% | 1.0 | 14 | 00.174228 | 802.11 Ack | FC=........ |
| 00:14:1B:5A:33:D0 | | 11 | 68% | 54.0 | 66 | 00.178863 | 802.1x | FC=.F......,SN=2871,FN= 0 |
| Aironet:A0:36:2F | | 11 | 58% | 1.0 | 282 | 00.200632 | EAP Response | FC=T.......,SN= 5,FN= 0 |
| Aironet:A0:36:2F | | 11 | 58% | 1.0 | 282 | 00.203340 | EAP Response | FC=T..R....,SN= 5,FN= 0 |
| 00:14:1B:5A:33:D0 | # | 11 | 71% | 1.0 | 14 | 00.203639 | 802.11 Ack | FC=........ |
| 00:14:1B:5A:33:D0 | | 11 | 70% | 54.0 | 188 | 00.207634 | 802.1x | FC=.F......,SN=2872,FN= 0 |
| Aironet:A0:36:2F | | 11 | 55% | 1.0 | 105 | 00.216295 | EAP Response | FC=T.......,SN= 6,FN= 0 |
| Aironet:A0:36:2F | | 11 | 57% | 1.0 | 105 | 00.217444 | EAP Response | FC=T..R....,SN= 6,FN= 0 |
| 00:14:1B:5A:33:D0 | # | 11 | 70% | 1.0 | 14 | 00.217754 | 802.11 Ack | FC=........ |
| 00:14:1B:5A:33:D0 | | 11 | 67% | 54.0 | 99 | 00.222799 | 802.1x | FC=.F......,SN=2874,FN= 0 |
| Aironet:A0:36:2F | | 11 | 55% | 1.0 | 152 | 00.254189 | EAP Response | FC=T.......,SN= 7,FN= 0 |
| 00:14:1B:5A:33:D0 | # | 11 | 68% | 1.0 | 14 | 00.254499 | 802.11 Ack | FC=........ |
| 00:14:1B:5A:33:D0 | | 11 | 64% | 54.0 | 147 | 00.288950 | 802.1x | FC=.F.R....,SN=2875,FN= 0 |
| Aironet:A0:36:2F | | 11 | 55% | 1.0 | 232 | 00.318087 | EAP Response | FC=T.......,SN= 8,FN= 0 |
| 00:14:1B:5A:33:D0 | # | 11 | 70% | 1.0 | 14 | 00.318383 | 802.11 Ack | FC=........ |
| 00:14:1B:5A:33:D0 | | 11 | 68% | 54.0 | 44 | 00.326833 | 802.1x | FC=.F......,SN=2877,FN= 0 |
| 00:14:1B:5A:33:D0 | | 11 | 65% | 54.0 | 44 | 00.326882 | 802.1x | FC=.F.R....,SN=2877,FN= 0 |
| 00:14:1B:5A:33:D0 | | 11 | 67% | 48.0 | 44 | 00.326922 | 802.1x | FC=.F.R....,SN=2877,FN= 0 |
| 00:14:1B:5A:33:D0 | | 11 | 67% | 54.0 | 157 | 00.326964 | 802.1x | FC=.F......,SN=2878,FN= 0 |
| Aironet:A0:36:2F | | 11 | 57% | 1.0 | 157 | 00.333742 | EAP01-Key | FC=T.......,SN= 9,FN= 0 |
| 00:14:1B:5A:33:D0 | # | 11 | 70% | 1.0 | 14 | 00.334019 | 802.11 Ack | FC=........ |
| 00:14:1B:5A:33:D0 | | 11 | 65% | 54.0 | 207 | 00.340467 | 802.1x | FC=.F......,SN=2879,FN= 0 |
| 00:14:1B:5A:33:D0 | | 11 | 67% | 54.0 | 207 | 00.341130 | 802.1x | FC=.F.R....,SN=2879,FN= 0 |
| Aironet:A0:36:2F | | 11 | 57% | 1.0 | 135 | 00.342542 | EAP01-Key | FC=T.......,SN= 10,FN= 0 |

Этот пакет показывает начальный ответ EAP EAP-FAST.

**Примечание:** Согласно конфигурации в клиенте CSSC, анонимном, используется в качестве внешней идентичности EAP в начальном ответе EAP.




## Отладка в контроллере беспроводной локальной сети

Эти команды отладки могут использоваться в контроллере беспроводной локальной сети для мониторинга выполнения опознавательного обмена:

- **debug aaa events enable**
- **подробность debug aaa включает**

- debug dot1x events enable
- состояния debug dot1x включают

Это - пример запуска опознавательной транзакции между клиентом CSSC и ACS, как проверено в контроллере беспроводной локальной сети с отладками:

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing RSN IE type 48,
   length 20 for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received RSN IE with
   0 PMKIDs from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
   moving mobile 00:40:96:a0:36:2f into Connecting state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-
   Request/Identity to mobile 00:40:96:a0:36:2f (EAP Id 1)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Identity Response
   (count=1) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f EAP State update from
   Connecting to Authenticating for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x - moving mobile
   00:40:96:a0:36:2f into Authenticating state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth
   Response state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AuthenticationRequest: 0x138dd764
Thu Aug 24 18:20:54 2006:       Callback.......0x10372764
Thu Aug 24 18:20:54 2006:       protocolType...0x00040001
Thu Aug 24 18:20:54 2006:       proxyState.....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006:       Packet contains 15 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Successful transmission of
   Authentication Packet (id 84) to 10.1.1.12:1812, proxy state0
Thu Aug 24 18:20:54 2006: ****Enter processIncomingMessages: response code=11
Thu Aug 24 18:20:54 2006: ****Enter processRadiusResponse: response code=11
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Access-Challenge received from
   RADIUS server 10.1.1.12 for mobile 00:40:96:a0:36:2f rec7
Thu Aug 24 18:20:54 2006: AuthorizationResponse: 0x11c8a394
Thu Aug 24 18:20:54 2006:       structureSize..147
Thu Aug 24 18:20:54 2006:       resultCode.....255
Thu Aug 24 18:20:54 2006:       protocolUsed...0x00000001
Thu Aug 24 18:20:54 2006:       proxyState.....00:40:96:A0:36:2F-11:00
Thu Aug 24 18:20:54 2006:       Packet contains 4 AVPs (not shown)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-Challenge
   for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth Req state
   (id=249) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f WARNING:
   updated EAP-Identifer 1 ===> 249 for STA 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP Request from
   AAA to mobile 00:40:96:a0:36:2f (EAP Id 249)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAP Response from
   mobile 00:40:96:a0:36:2f (EAP Id 249, EAP Type 3)
```

Это - успешное завершение обмена EAP от отладки контроллера (с аутентификацией WPA2):

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-
   Accept for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Applying new AAA
   override for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Override values for station
   00:40:96:a0:36:2f source: 4, valid bits: 0x0
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout:
   -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, r1'
```

```
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Unable to apply override
   policy for station 00:40:96:a0:36:2f - VapAllowRadiusOverride E
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Creating a new PMK Cache Entry
   for station 00:40:96:a0:36:2f (RSN 2)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Adding BSSID
   00:14:1b:5a:33:d0 to PMKID cache for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: New PMKID: (16)
Thu Aug 24 18:20:54 2006:      [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b
   72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-Success
   to mobile 00:40:96:a0:36:2f (EAP Id 0)
Thu Aug 24 18:20:54 2006: Including PMKID in M1  (16)
Thu Aug 24 18:20:54 2006:
   [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b 72 1f 3f 5f 5b
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message to
   mobile 00:40:96:a0:36:2f state INITPMK (message 1), repl0
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend
   Auth Success state (id=0) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Auth Success
   while in Authenticating state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x -
   moving mobile 00:40:96:a0:36:2f into Authenticated state
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-
   Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version
   (1) in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key
   in PKT_START state (message 2) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Stopping retransmission
   timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message
   to mobile 00:40:96:a0:36:2f state PTKINITNEGOTIATING (messa1
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received
   EAPOL-Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version (1)
   in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key in
   PTKINITNEGOTIATING state (message 4) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AccountingMessage
   Accounting Interim: 0x138dd764
Thu Aug 24 18:20:54 2006: Packet contains 20 AVPs:
Thu Aug 24 18:20:54 2006:
   AVP[01] User-Name.................enterprise (10 bytes)
Thu Aug 24 18:20:54 2006: AVP[02]
   Nas-Port..........................0x0000001d (29) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[03]
   Nas-Ip-Address....................0x0a0a5003 (168448003) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[04]
   Class.............................CACS:0/28b5/a0a5003/29 (22 bytes)
Thu Aug 24 18:20:54 2006: AVP[05]
   NAS-Identifier....................ws-3750 (7 bytes)
Thu Aug 24 18:20:54 2006: AVP[06]
   Airespace / WLAN-Identifier........0x00000001 (1) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[07]
   Acct-Session-Id...................44ede3b0/00:40:
   96:a0:36:2f/14 (29 bytes)
Thu Aug 24 18:20:54 2006: AVP[08]
   Acct-Authentic....................0x00000001 (1) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[09]
   Tunnel-Type.......................0x0000000d (13) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[10]
   Tunnel-Medium-Type................0x00000006 (6) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[11]
   Tunnel-Group-Id...................0x3832 (14386) (2 bytes)
```

```
Thu Aug 24 18:20:54 2006: AVP[12]
   Acct-Status-Type.................0x00000003 (3) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[13]
   Acct-Input-Octets................0x000b99a6 (760230) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[14]
   Acct-Output-Octets...............0x00043a27 (277031) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[15]
   Acct-Input-Packets...............0x0000444b (17483) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[16]
   Acct-Output-Packets..............0x0000099b (2459) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[17]
   Acct-Session-Time................0x00000a57 (2647) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[18]
   Acct-Delay-Time..................0x00000000 (0) (4 bytes)
Thu Aug 24 18:20:54 2006: AVP[19]
   Calling-Station-Id...............10.10.82.11 (11 bytes)
Thu Aug 24 18:20:54 2006: AVP[20]
   Called-Station-Id................10.10.80.3 (10 bytes)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f
   Stopping retransmission timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:57 2006: User admin authenticated
```

## Дополнительные сведения

- Руководство по установке для Cisco Secure ACS для Windows Server
- Руководство по конфигурации для Cisco Secure ACS 4.1
- Пример настройки ограничения доступа к WLAN на основе SSID с WLC и Cisco Secure ACS
- EAP-TLS в Unified Wireless Network с ACS 4.0 и Windows 2003
- Пример конфигурации "Dynamic VLAN Assignment with RADIUS Server and Wireless LAN Controller"
- Cisco Systems – техническая поддержка и документация