Пример конфигурации локальной проверки подлинности EAP на контроллере беспроводных LAN с EAP-FAST и сервером LDAP

Содержание

Введение

Этот документ объясняет, как настроить Протокол EAP - Гибкая Аутентификация через Безопасный, Туннелирующий (FAST) Локальная EAP-аутентификация на Контроллере беспроводной локальной сети (WLC). В нем также поясняется настройка сервера LDAP в качестве служебной базы данных для получения реквизитов пользователя и выполнения аутентификации пользователя в локальном режиме EAP.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Cisco WLC серии 4400, который выполняет микропрограммное обеспечение 4.2
- Cisco Aironet облегченная точка доступа (LAP) серии 1232AG
- Microsoft Windows 2003 Server, настроенный как контроллер домена, Сервер LDAP, а также сервер Центра сертификации.
- Клиентский адаптер a/b/g 802.11 Cisco Aironet, который выполняет релиз микропрограммы 4.2
- Утилита Cisco Aironet Desktop Utility (ADU), которая выполняет версию микропрограммы 4.2

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

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

Общие сведения

Локальная EAP-аутентификация на Контроллерах беспроводной локальной сети была начата с версии 4.1.171.0 Контроллера беспроводной локальной сети.

Локальный EAP является методом аутентификации, который позволяет пользователям и беспроводным клиентам аутентифицироваться локально на контроллере. Он разработан для работы в удаленных офисах, которым необходимо поддерживать подключение к беспроводным клиентам, если нарушена связь с внутренней системой, или внешний сервер аутентификации перестал работать. При включении локального EAP контроллер служит сервером проверки подлинности и базой локальных пользователей, таким образом, это удаляет зависимость от внешнего сервера проверки подлинности. Чтобы выполнить аутентификацию пользователя, локальный EAP извлекает учетные данные пользователя из локальной базы данных пользователя или внутренней базы данных LDAP. Локальный EAP поддерживает LEAP, EAP-FAST, EAP-TLS, P EAPv0/MSCHAPv2 и аутентификацию PEAPv1/GTC между контроллером и беспроводными клиентами.

Локальный EAP может использовать Сервер LDAP в качестве своей базы данных бэкэнда для получения учетных данных пользователя.

База данных бэкэнда LDAP позволяет контроллеру сделать запрос Сервера LDAP для учетных данных (имя пользователя и пароль) индивидуального пользователя. Эти учетные данные тогда используются для аутентификации пользователя.

Поддержка БД бэкэнда LDAP эти Локальные методы EAP:

- EAP-FAST / GTC
- EAP-TLS
- PEAPv1/GTC.

LEAP, EAP-FAST/MSCHAPv2, и PEAPv0/MSCHAPv2 также поддерживаются, **но только если Сервер LDAP установлен для возврата нешифрованного пароля**. Например, Microsoft Active Directory не поддерживается, потому что она не возвращает нешифрованный пароль. Если Сервер LDAP не может быть настроен для возврата нешифрованного пароля, LEAP, EAP-FAST/MSCHAPv2, и PEAPv0/MSCHAPv2 не поддерживаются.

Примечание: Если какие-либо серверы RADIUS настроены на контроллере, контроллер пытается аутентифицировать беспроводных клиентов, использующих серверы RADIUS сначала. Локальный EAP выполняет попытку аутентифицировать пользователей, только если серверы RADIUS не обнаружены, устарели или не настроены. Если четыре сервера RADIUS настроены, контроллер пытается аутентифицировать клиента с первым сервером RADIUS, то второй сервер RADIUS, и затем локальный EAP. Если клиент пытается тогда повторно аутентифицироваться вручную, контроллер пробует третий сервер RADIUS, то четвертый сервер RADIUS, и затем локальный EAP.

Данный пример использует EAP-FAST в качестве Локального метода EAP на WLC, который в свою очередь настроен для запроса базы данных бэкэнда LDAP для учетных данных пользователя беспроводного клиента.

Настройка

Этот документ использует EAP-FAST с сертификатами и на клиенте и на стороне сервера. Для этого настройка использует **Microsoft Certificate Authority (CA)** сервер для генерации сертификатов клиента и сервера.

Учетные данные пользователя сохранены в Сервере LDAP так, чтобы на успешном подтверждении сертификата, контроллер делал запрос Сервера LDAP, чтобы получить учетные данные пользователя и аутентифицирует беспроводного клиента.

Этот документ предполагает, что эти конфигурации уже на месте:

- LAP зарегистрирован к WLC. См. регистрацию облегченных точек доступа к Контроллеру беспроводной локальной сети (WLC) для получения дополнительной информации о процессе регистрации.
- Сервер DHCP настроен для присвоения IP-адреса на беспроводных клиентов.
- Microsoft Windows 2003 Server настроен как контроллер домена, а также CA сервер. Данный пример использует **wireless.com** в качестве домена.Именуйте Windows 2003 Настройки как Контроллер домена для получения дополнительной информации о настройке Windows 2003 Server как контроллер домена.См. Установку и Настраивают Microsoft Windows 2003 Server как Сервер Центра сертификации (CA) для настройки Windows 2003 Server как Предприятие CA сервер.

Схема сети

В настоящем документе используется следующая схема сети:

Конфигурации

Выполните эти шаги для реализации этой конфигурации:

- Настройте EAP-FAST как метод локальной EAP-аутентификации на WLC
- Настройте сервер LDAP
- Настройте беспроводного клиента

Настройте EAP-FAST как метод локальной EAP-аутентификации на WLC

Как отмечалось ранее, этот документ использует EAP-FAST с сертификатами и на клиенте и на стороне сервера как метод Локальной EAP-аутентификации. Первый шаг должен загрузить и установить следующие сертификаты к серверу (WLC, в этом случае) и клиент.

WLC и клиент каждая потребность эти сертификаты, которые будут загружены от сервера CA:

- Сертификат устройства (один для WLC и один для клиента)
- Корневой сертификат Инфраструктуры открытых ключей (PKI) для WLC и Сертификата CA для клиента

Генерируйте сертификат устройства для WLC

Выполните эти шаги для генерации сертификата устройства для WLC от сервера CA. Этот сертификат устройства используется WLC для аутентификации на клиенте.

1. Перейдите **к http://адрес <IP server> CA/certsrv** от вашего ПК, который имеет сетевое подключение к серверу CA. Войдите как администратор сервера CA.
2. Выберите **Request сертификат**.
3. На странице Request a Certificate нажмите **усовершенствованный запрос сертификата**.
4. На странице Advanced Certificate Request нажмите **Create и отправьте запрос к этому CA.**, Это берет вас к Усовершенствованной форме запроса сертификата.
5. В Усовершенствованной Форме запроса сертификата выберите **Web Server** в качестве Шаблона сертификата. Затем задайте название к этому сертификату устройства.Данные примеры используют название сертификата в качестве ciscowlc123. Заполните другую информацию об определении согласно своему требованию.
6. Под **Ключевым** разделом **Опций** выберите **Mark Keys как экспортируемый параметр**. Иногда, этот определенный параметр отобразится серым и не может быть включен или отключен при выборе шаблона веб-сервера. В таких случаях нажмите **Back** из меню браузера, чтобы пойти одна страница назад и снова возвратиться к этой странице. На этот раз Ключи Марка как экспортируемый параметр должны быть доступными.

7. Настройте все другие необходимые поля и нажмите **Submit**.
8. Нажмите **Yes** в следующем окне для разрешения процесса запроса сертификата.
9. Окно Certificate Issued появляется, который указывает на успешный процесс запроса сертификата. Следующий шаг должен установить выполненный сертификат к хранилищу сертификата этого ПК. **Нажмите кнопку Install this certificate (Установить этот сертификат).**
10. Новый сертификат установлен успешно к ПК от того, где запрос генерируется к серверу CA.
11. Следующий шаг должен экспортировать этот сертификат с хранилища сертификата на жесткий диск как файл. Этот файл сертификата будет позже использоваться для загрузки сертификата к WLC.Для экспортирования сертификата от хранилища сертификата откройте браузер Internet Explorer, затем нажмите **Tools> Internet Options**.
12. Нажмите **Content> Certificates**, чтобы перейти к хранилищу сертификата, где сертификаты установлены по умолчанию.
13. Сертификаты устройства обычно устанавливаются под списком **Персонального сертификата**. Здесь, необходимо видеть новый установленный сертификат. Выберите сертификат и нажмите **Export**.
14. Нажмите **Next** в следующих окнах. Выберите **Yes, экспортируйте** опцию **с закрытым ключом** в **Окне мастера Экспорта Сертификата**. **Нажмите кнопку Next.**
15. Выберите формат файла экспорта в качестве**.PFX** и выберите опцию **надежной защиты Enable**. **Нажмите кнопку Next.**
16. В Окне ввода пароля введите пароль. Данный пример использует **Cisco** в качестве пароля.
17. Сохраните файл сертификата (файл.PFX) к вашему жесткому диску. Нажмите **Next** и закончите процесс экспорта успешно.

Загрузка Сертификата устройства на WLC

Теперь, когда сертификат устройства WLC доступен как файл.PFX, следующий шаг должен загрузить файл к контроллеру. WLC Cisco принимают сертификаты только в формате.PEM. Поэтому необходимо сначала преобразовать.PFX или файл формата PKCS12 к файлу PEM с помощью openSSL программы.

Преобразуйте Сертификат в PFX к Формату PEM Использование openSSL Программы

Можно скопировать сертификат к любому ПК, где у вас есть openSSL, установленный для преобразования его в формат PEM. Введите эти команды в файл Openssl.exe в папке bin openSSL программы:

Примечание: Можно загрузить openSSL от веб-сайта OpenSSL.

```
openssl>pkcs12 -in ciscowlc123.pfx -out ciscowlc123.pem !--- ciscowlc123 is the name used in this example for the exported file. !--- You can specify any name to your certificate file.
Enter Import Password : cisco !--- This is the same password that is mentioned in step 16 of the previous section. MAC verified Ok Enter PEM Pass phrase : cisco !--- Specify any passphrase here. This example uses the PEM passphrase as cisco. Verifying - PEM pass phrase : cisco
```

Файл сертификата преобразован в формат PEM. Следующий шаг должен загрузить сертификат устройства форматирования PEM к WLC.

Примечание: Перед этим вам нужно программное обеспечение сервера TFTP на вашем ПК

от того, где файл PEM будет загруженным. Этот ПК должен иметь подключение к WLC. Сервер TFTP должен иметь свой текущий и основной каталог, заданный с местоположением, где хранится файл PEM.

Загрузите преобразованный сертификат устройства форматирования PEM к WLC

Данный пример объясняет процесс загрузки через CLI WLC.

1. Вход в систему к CLI контроллера.
2. Введите **команду transfer download datatype eapdevcert**.
3. Введите **transfer download serverip** *10.77.244.196* команды.10.77.244.196 IP-адрес сервера TFTP.
4. Введите **transfer download filename** *ciscowlc.pem* команда.ciscowlc123.pem является именем файла, используемым в данном примере.
5. Введите **команду transfer download certpassword** для установки пароля для сертификата.
6. Введите **команду transfer download start** для просмотра обновленных настроек.Затем ответ **y**, когда предложено подтвердить текущие параметры и запустить процесс загрузки.Данный пример показывает выходные данные команды загрузки:
```
(Cisco Controller) >transfer download start Mode..... TFTP
Data Type..... Vendor Dev Cert TFTP Server
IP..... 10.77.244.196 TFTP Packet
Timeout..... 6 TFTP Max Retries.....
10 TFTP Path..... TFTP
Filename..... ciscowlc.pem This may take some time. Are you
sure you want to start? (y/N) y TFTP EAP CA cert transfer starting. Certificate installed.
Reboot the switch to use the new certificate. Enter the reset system command to reboot the
controller. The controller is now loaded with the device certificate.
```
7. Введите **команду reset system** для перезагрузки контроллера. Контроллер теперь загружен сертификатом устройства.

Установите корневой сертификат PKI в WLC

Теперь, когда сертификат устройства установлен в WLC, следующий шаг должен установить Корневой сертификат PKI к WLC от сервера CA. Выполните данные действия:

1. Перейдите **к http://адрес <IP server> CA/certsrv** от вашего ПК, который имеет сетевое подключение к серверу CA. Вход в систему как администратор сервера CA.
2. Нажмите **Download a CA certificate, цепочку сертификатов или CRL**.
3. На результирующей странице вы видите текущие сертификаты CA, доступные на сервере CA под коробкой **сертификата CA**. Выберите **DER** в качестве Способа кодирования и нажмите **Download CA certificate**.
4. Сохраните сертификат как **.cer** файл. Данный пример использует **certnew.cer** в качестве имени файла.
5. Следующий шаг должен преобразовать .cer файл в формат PEM и загрузить его к контроллеру. Для выполнения этих шагов повторите ту же процедуру, объясненную в Загрузке Сертификата устройства к разделу WLC с этими изменениями:openSSL "-в" и "-" файлы являются **certnew.cer** и **certnew.pem**.Кроме того, никакая Фраза - пропуск PEM или пароли импорта не требуются в этом процессе.Кроме того, openSSL команда для преобразования **.cer** файла в файл **.pem**:**x509 - в** *certnew.cer* **- сообщают DER** -

certnew.pem-**outform PEM**В шаге 2 Загрузки Преобразованный Сертификат Устройства форматирования PEM к разделу WLC команда для загрузки сертификата к WLC:(Cisco Controller)> **transfer download datatype eapcacert**Файл, который будет загружен к WLC, является **certnew.pem**.

Можно проверить, установлены ли сертификаты на WLC от графического интерфейса контроллера следующим образом:

- От GUI WLC нажмите **Security**. На странице Security нажмите **Advanced> IPSec Certs** от задач, которые появляются слева. Нажмите **CA Certificate** для просмотра установленного сертификата CA. Ниже представлен пример:
- Чтобы проверить, установлен ли сертификат устройства на WLC от GUI WLC, нажмите **Security**. На странице Security нажмите **Advanced> IPSec Certs** от задач, которые появляются слева. Нажмите **ID Certificate** для просмотра установленного сертификата устройства. Ниже представлен пример:

Генерируйте сертификат устройства для клиента

Теперь, когда сертификат устройства и сертификат CA установлены на WLC, следующий шаг должен генерировать эти сертификаты для клиента.

Выполните эти шаги для генерации сертификата устройства для клиента. Этот сертификат будет использоваться клиентом для аутентификации на WLC. Этот документ объясняет шаги, вовлеченные в генерацию сертификатов для клиента Windows XP Professional.

1. Перейдите **к http://адрес <IP server> CA/certsrv** от клиента, который требует, чтобы был установлен сертификат. Вход в систему как домен name\username к серверу CA. Имя пользователя должно быть именем пользователя, который использует эту машину XP, и пользователь должен уже быть настроен как часть того же домена как сервер CA.
2. Выберите **Request сертификат**.
3. На странице Request a Certificate нажмите **усовершенствованный запрос сертификата**.
4. На странице Advanced Certificate Request нажмите **Create и отправьте запрос к этому CA.**, Это берет вас к Усовершенствованной Форме запроса сертификата.
5. В Усовершенствованной Форме запроса сертификата выберите **User** из раскрывающегося меню Шаблона сертификата.Под разделом опций Key выберите эти параметры:Введите поле Key Sizein the Key Size. Данный пример использует **1024**.Проверьте **Ключи Марка как экспортируемый параметр**.
6. Настройте все другие необходимые поля и нажмите **Submit**.
7. Сертификат устройства клиента теперь генерируется согласно запросу. Нажмите **Install сертификат** для установки сертификата к хранилищу сертификата.
8. Должна существовать возможность для обнаружения сертификата устройства клиента установленным под Персональным сертификатом перечисляют под **Программными средствами> интернет-Опции> Содержание> Сертификаты** на браузере IE клиента.Сертификат устройства для клиента установлен на клиенте.

Генерируйте корневой сертификат CA для клиента

Следующий шаг должен генерировать сертификат CA для клиента. Выполните эти шаги от клиентского компьютера:

1. Перейдите **к http://адрес <IP server> CA/certsrv** от клиента, который требует, чтобы был установлен сертификат. Вход в систему как домен name\username к серверу CA. Имя пользователя должно быть именем пользователя, который использует эту машину XP, и пользователь должен уже быть настроен как часть того же домена как сервер CA.
2. На результирующей странице вы видите текущие сертификаты CA, доступные на сервере CA под коробкой **сертификата CA**. Выберите **Base 64** в качестве Способа кодирования. Затем нажмите **Download CA certificate** и сохраните файл к ПК клиента как **.cer** файл. Данный пример использует **rootca.cer** в качестве имени файла.
3. Затем, установите .cer формат сертификата CA, в котором сохраняют, к хранилищу сертификата клиента. Двойное нажатие на rootca.cer файле и нажимает **Install Certificate**.
4. Нажмите **Next** для импорта сертификата от жесткого диска клиента до хранилища сертификата.
5. Выберите **Automatically выбирают хранилище сертификата на основе типа сертификата** и нажимают **Next**.
6. Нажмите **Finish** для завершения процесса Импорта.
7. По умолчанию сертификаты CA установлены под списком Доверенных корневых центров сертификации на браузере IE клиента под **Программными средствами> интернет-Опции> Содержание> Сертификаты**. Ниже представлен пример:

Все требуемые сертификаты установлены на WLC, а также клиенте для Локальной EAP-аутентификации EAP-FAST. Следующий шаг должен настроить WLC для Локальной EAP-аутентификации.

Настройте локальный EAP на WLC

Выполните эти шаги от **режима GUI WLC** для настройки Локальной EAP-аутентификации на WLC:

1. Нажмите **Security> Local EAP**.
2. Под Локальным EAP нажмите **Profiles** для настройки Локального EAP profile.
3. Нажмите **New** для создания нового Локального EAP profile.
4. Настройте название для этого профиля и нажмите **Apply**. В данном примере имя профиля является **ldap**. Это берет вас к Локальному Eap profile, созданному на WLC.
5. Нажмите профиль **ldap**, который был просто создан, который появляется под полем Profile Name страницы Local EAP Profiles. Это берет вас к **Локальному Eap profile> страница Edit**.
6. Настройте параметры, определенные для этого профиля на **Локальном Eap profile> страница Edit**.Выберите **EAP-FAST** в качестве метода Локальной EAP-аутентификации.Включите флажки рядом с **Локальным Требуемым Сертификатом** и **Требуемый Сертификат клиента**.Выберите **Vendor** в качестве Отправителя Сертификата, потому что этот документ использует третью сторону CA сервер.Позвольте флажку затем **Проверить против сертификатов CA**, чтобы позволить входящему сертификату от клиента быть проверенным против сертификатов CA на контроллере.Если вы хотите, чтобы общее имя (CN) во входящем сертификате было проверено против CN сертификатов CA на контроллере, установите **Сверять** флажок **Установления личности CN Сертификата**. По умолчанию эта функция отключена. Чтобы позволить контроллеру проверять, что входящий сертификат устройства все еще допустим и не истек, установите флажок **Проверки достоверности Даты**

Сертификата Проверки.**Примечание:** Законность даты сертификата проверена против текущего UTC (GMT) время, которое настроено на контроллере. Смещение часового пояса проигнорировано.**Щелкните "Применить".**

7. Локальный EAP profile с аутентификацией EAP-FAST теперь создан на WLC.
8. Следующий шаг должен настроить EAP-FAST определенные параметры на WLC. На странице WLC Security нажмите **Local EAP> EAP-FAST Parameters** для перемещения в страницу EAP-FAST Method Parameters.Анчек флажок **Anonymous Provision**, потому что данный пример объясняет EAP-FAST с помощью сертификатов. Оставьте все другие параметры в их настройках по умолчанию. **Щелкните "Применить".**

Настройте WLC с подробными данными сервера LDAP

Теперь, когда WLC настроен с Локальным EAP profile и дополнительными сведениями, следующий шаг должен настроить WLC с подробными данными Сервера LDAP. Выполните эти шаги на WLC:

1. На странице **Security** WLC выберите **AAA> LDAP** от панели задач левой части для перемещения в страницу конфигурации Сервера LDAP. Для добавления Сервера LDAP нажмите **New**. Страница **LDAP Servers> New** появляется.
2. На странице Edit Серверов LDAP задайте подробные данные Сервера LDAP, такие как IP-адрес Сервера LDAP, Номера порта, Включите Состояние сервера и так далее.Выберите номер из **Индекса Сервера (Приоритетное)** раскрывающееся окно для определения порядка приоритетов этого сервера относительно любых других настроенных Серверов LDAP. Можно настроить до семнадцати серверов. Если контроллер не может достигнуть первого сервера, он пробует второй в списке и так далее.Введите IP-адрес Сервера LDAP в поле **Server IP Address**.Введите номер порта TCP Сервера LDAP в поле **Port Number**. Допустимый диапазон 1 - 65535, и значение по умолчанию **389**.В поле **User Base DN** введите составное имя (DN) поддерева в Сервере LDAP, который содержит список всех пользователей. Например, ou=organizational модуль, .ou=next подразделение и o=corporation.com. Если дерево, содержащее пользователей, является основным DN, введите o=corporation.com или dc=corporation, dc=com.В данном примере пользователь расположен под Подразделением (OU) **ldapuser**, который в свою очередь создан как часть домена **Wireless.com**.DN Пользовательской базы должен указать полный путь, где расположены сведения о пользователе (мандат пользователя согласно методу аутентификации EAP-FAST). В данном примере пользователь расположен под основным DN OU=ldapuser, DC=Wireless, DC=com.Больше подробных данных о OU, а также пользовательской конфигурации, объяснено в Пользователях Создания на разделе Контроллера домена этого документа.В поле **User Attribute** введите имя атрибута в записи пользователя, которая содержит имя пользователя.В поле **User Object Type** введите значение атрибута LDAP objectType, который определяет запись как пользователя. Часто, записи пользователя имеют несколько значений для атрибута objectType, некоторые из которых уникальны для пользователя и некоторые из которых разделены с другими типами объекта.**Примечание:** Можно получить значение этих двух полей от сервера каталогов с утилитой браузера LDAP, которая стала частью инструментов поддержки Windows 2003. **Это программное средство браузера Microsoft LDAP называют LDP.** С помощью этого программного средства можно знать DN Пользовательской базы, Атрибут пользователя и поля User Object Type этого

индивидуального пользователя. Подробные сведения об использовании LDP для знания их Пользователь определенные атрибуты обсуждены в Использовании LDP для Определения раздела Атрибутов пользователя этого документа.Выберите **Secure** из раскрывающегося окна Режима сервера, если вы хотите, чтобы все транзакции LDAP использовали безопасный туннель TLS. В противном случае выберите **None**, который является настройкой по умолчанию.В поле **Server Timeout** введите кол-во секунд между повторными передачами. Допустимый диапазон составляет 2 - 30 секунд, и значение по умолчанию составляет 2 секунды.Проверьте флажок **Enable Server Status**, чтобы включить этот Сервер LDAP или снять флажок с ним для отключения. Значение по умолчанию отключено.Нажмите **Apply** для фиксации изменений.Вот пример, уже настроенный с этой информацией:Теперь, когда подробные данные о Сервере LDAP настроены на WLC, следующий шаг должен настроить LDAP как приоритетную базу данных бэкэнда так, чтобы WLC сначала смотрел на базу данных LDAP для учетных данных пользователя, а не любых других баз данных.

Настройте LDAP как приоритетную базу данных бэкэнда

Выполните эти шаги на WLC для настройки LDAP как приоритетной базы данных бэкэнда:

1. На странице Security нажмите **Local EAP> Authentication Priority**. В Порядке приоритетов> страница Local-Auth, можно найти две базы данных (Локальный и LDAP), который может сохранить учетные данные пользователя.Для создания LDAP как приоритетной базы данных выберите **LDAP** из коробки учетных данных пользователя левой части и нажмите**>** кнопка для перемещения LDAP в коробку порядка приоритетов на правой части.
2. Данный пример ясно иллюстрирует, что LDAP выбран на коробке левой части и**>**, кнопка нажата. Как результат, LDAP перемещен в коробку на правой части, которая решает приоритет. База данных LDAP выбрана в качестве базы данных Приоритета аутентификации.**Щелкните "Применить".Примечание:** Если и LDAP и ЛОКАЛЬНЫЙ появляется в коробке Учетных данных подходящего пользователя с LDAP на главном и ЛОКАЛЬНЫМ на нижней части, Локальный EAP пытается аутентифицировать клиентов, использующих базу данных бэкэнда LDAP и переключения при отказе к базе локальных пользователей, если Серверы LDAP не достижимы. Если пользователь не найден, попытка аутентификации отклонена. Если ЛОКАЛЬНЫЙ находится на главных, Локальных попытках EAP к используемой аутентификации только база локальных пользователей. Это не переключается при отказе к базе данных бэкэнда LDAP.

Настройте WLAN на WLC с локальной EAP-аутентификацией

Последний шаг в WLC должен настроить WLAN, который использует Локальный EAP в качестве его метода аутентификации с LDAP как его база данных бэкэнда. Выполните данные действия:

1. Из Главного меню Контроллера нажмите **WLAN** для перемещения в страницу конфигурации WLAN. В странице WLANs нажмите **New** для создания нового WLAN. Данный пример создает новый **ldap** WLAN.Нажмите следующий шаг **Apply The** должен настроить параметры WLAN в WLAN> страница Edit.
2. На странице edit WLAN включите статус этого WLAN. Настройте все другие

обязательные параметры.
3. Нажмите **Security** для настройки связанных параметров безопасности для этого WLAN. Данный пример использует безопасность уровня 2 в качестве 802.1x с динамическим WEP на 104 бита.**Примечание:** Этот документ использует 802.1x с динамическим WEP как пример. Рекомендуется использовать больше методов безопасной аутентификации, таких как WPA / WPA2.
4. В странице конфигурации Безопасности беспроводных сетей нажмите **theAAA** вкладку **серверов**. На странице AAA-серверов включите метод Локальной EAP-аутентификации и выберите **ldap** из раскрывающегося окна, которое соответствует параметру Названия EAP Profile. Это - Локальный EAP profile, созданный в данном примере.
5. Выберите Сервер LDAP (который был ранее настроен на WLC) от раскрывающегося окна. Удостоверьтесь, что Сервер LDAP достижим от WLC.**Щелкните "Применить".**
6. Новый WLAN **ldaphas** настроенный на WLC. Этот WLAN аутентифицирует клиентов с Локальной EAP-аутентификацией (EAP-FAST в этом случае) и делает запрос базы данных бэкэнда LDAP для клиентской учетной проверки.

Настройте сервер LDAP

Теперь, когда Локальный EAP настроен на WLC, следующий шаг должен настроить Сервер LDAP, который служит базой данных бэкэнда для аутентификации беспроводных клиентов на успешное подтверждение сертификата.

Первый шаг в настройке Сервера LDAP должен создать базу данных пользователей на Сервере LDAP так, чтобы WLC мог сделать запрос этой базы данных для аутентификации пользователя.

Создание пользователей на контроллере домена

В данном примере создан новый OU **ldapuser**, и пользователь **user2** создан под этим OU. Путем настройки этого пользователя для доступа LDAP WLC может сделать запрос этой базы данных LDAP для проверки подлинности пользователя.

Домен, используемый в данном примере, является **wireless.com**.

Создайте базу данных пользователей под OU

Этот раздел объясняет, как создать новый OU в вашем домене и создать нового пользователя на этом OU.

1. В контроллере домена нажмите **Start> Programs> Administrative Tools> Active Directory Users and Computers** для запуска консоли управления **Пользователей и компьютеров Active Directory**.
2. Щелкните правой кнопкой мыши на своем доменном имени (wireless.com, в данном примере), затем выберите **New> Organizational Unit** из контекстного меню для создания нового OU.
3. Назначьте название к этому OU и нажмите **OK**.

Теперь, когда новый OU **ldapuser** создан на Сервере LDAP, следующий шаг должен создать пользователя **user2** под этим OU. Для достижения этого выполните эти шаги:

1. Щелкните правой кнопкой мыши на новом созданном OU. Выберите **New> User** из результирующих контекстных меню для создания нового пользователя.
2. На странице Настройки пользователя заполните обязательные поля как показано в данном примере. Данный пример имеет **user2** как Пользовательское имя пользователя.Это - имя пользователя, которое будет проверено в базе данных LDAP для аутентификации клиента. Данный пример использует **abcd** в качестве Имени и Фамилии. **Нажмите кнопку Next.**
3. Введите пароль и подтвердите пароль. Выберите **Password никогда не истекает** опцию, и нажмите **Next**.
4. **Нажмите кнопку Finish.**Новый пользователь **user2** создан под OU **ldapuser**. Учетные данные пользователя:username: **user2**password: **Laptop123**

Теперь, когда пользователь под OU создан, следующий шаг должен настроить этого пользователя для доступа LDAP.

Настройте пользователя для доступа LDAP

Выполните шаги в этот раздел для настройки пользователя для доступа LDAP.

Включите анонимный, связывают функцию на Windows 2003 Server

Для любых приложений от стороннего разработчика для доступа к Windows 2003 AD на LDAP Анонимные Связывают функцию, должен быть включен на Windows 2003. По умолчанию анонимные операции LDAP не разрешены на контроллерах домена Windows 2003.

Выполните эти шаги для включения Анонимный, Связывают функцию:

1. Запуск **ADSI Редактирует** программное средство от Пуска> Выполнить местоположения> Тип: **ADSI Edit.msc**. Это программное средство является частью инструментов поддержки Windows 2003.
2. В Окне редактирования ADSI разверните Корневой домен (Конфигурация [tsweb-lapt. Wireless.com]).Разверните **CN=Services> NT CN=Windows> Сервис CN=Directory**. Щелкните правой кнопкой мыши **Контейнер служб CN=Directory** и выберите **свойства** из контекстного меню.
3. В **Сервисном Окне свойств CN=Directory** нажмите атрибут **dsHeuristics** под полем Attribute и выберите **Edit**. В окне **String Attribute Editor** этого атрибута введите значение **0000002** и нажмите **Apply** и **OK**. Анонимные Связывают функцию, включен на Windows 2003 Server.**Примечание:** Последний (седьмой) символ является тем, который управляет способом, которым можно связать с сервисом LDAP. "0" или никакой седьмой символ означает, что отключены анонимные операции LDAP. **Установка седьмого символа к "2" включает Анонимный, Связывают функцию.Примечание:** Если этот атрибут уже содержит значение, удостоверьтесь, что вы изменяете только седьмой символ слева. Это - единственный символ, который должен быть изменен для включения анонимный, связывает. Например, если текущее значение будет "0010000", то необходимо будет изменить его на "0010002". Если текущее значение составит меньше чем семь символов, то необходимо будет поместить нули в места, не используемые: "001" станет "0010002".

Предоставление доступа ВХОДА В СИСТЕМУ ANONYMOUS пользователю "user2"

Следующий шаг должен предоставить доступ **ВХОДА В СИСТЕМУ ANONYMOUS** пользователю **user2**. Выполните эти шаги для достижения этого:

1. **Откройте службу Active Directory Users and Computers.**
2. Удостоверьтесь, что проверены **Обзорные Дополнительные характеристики**.
3. Перейдите пользователю **user2** и щелкните правой кнопкой мыши его. Выберите **Properties** из контекстного меню. Этот пользователь определен с именем "abcd".
4. Перейдите **к Безопасности** в abcd Окне свойств.
5. **Нажмите Add** в результирующем окне.
6. Введите **ВХОД В СИСТЕМУ ANONYMOUS** при **Введении имен объекта, чтобы выбрать** коробку и подтвердить диалоговое окно.
7. В ACL вы заметите, что **ВХОД В СИСТЕМУ ANONYMOUS** имеет доступ к некоторым наборам свойств пользователя. **Нажмите кнопку ОК**. Доступ ВХОДА В СИСТЕМУ ANONYMOUS предоставлен на этом пользователе.

[Давание разрешения содержания списка на OU]

Следующий шаг должен дать, по крайней мере, разрешение **Содержания Списка** к **ВХОДУ В СИСТЕМУ ANONYMOUS** на OU, что расположен пользователь. В данном примере "user2" расположен на OU "ldapuser". Выполните эти шаги для достижения этого:

1. В Пользователях и компьютерах Active Directory щелкните правой кнопкой мыши OU **ldapuser** и выберите **Properties**.
2. Нажмите **Security** и затем **Усовершенствованный**.
3. **Нажмите Add.** В диалоговом окне, которое открывается, введите **ВХОД В СИСТЕМУ ANONYMOUS**.
4. Подтвердите диалоговое окно. Это открывает новое диалоговое окно.
5. В **Применении на** раскрывающееся окно выберите **This object только** и включите флажок Allow **Содержания Списка**.

Использование LDP для определения атрибутов пользователя

Это программное средство GUI является клиентом LDAP, который позволяет пользователям выполнять операции (такие как подключение, свяжите, ищите, модифицируйте, добавьте, удалите) против любого совместимого с LDAP каталога, такого как Active Directory. LDP используется к объектам view, сохраненным в Active Directory наряду с их метаданными, таким как метаданные репликации и дескрипторы безопасности.

Программное средство GUI LDP включено при установке Инструментов поддержки Windows Server 2003 от CD продукта. Этот раздел объясняет использование утилиты LDP для определения определенных атрибутов, привязанных к пользователю **user2**. Некоторые из этих атрибутов используются для заполнения параметров конфигурации Сервера LDAP на WLC, таких как тип Атрибута пользователя и тип Объекта пользователя.

1. На Windows 2003 Server (даже на том же Сервере LDAP), нажмите **Start> Run** и

введите **LDP** для доступа к браузеру LDP.
2. В главном окне LDP нажмите **Connection> Connect** и подключение к Серверу LDAP путем ввода IP-адреса Сервера LDAP.
3. После того, как связанный с Сервером LDAP, выберите **View** из главного меню и нажмите **Tree**.
4. В результирующем окне Tree View введите BaseDN пользователя. В данном примере **user2 расположен под OU "ldapuser" под доменным Wireless.com**. Поэтому BaseDN для пользователя **user2** является **OU=ldapuser, dc=wireless, dc=com**. **Нажмите кнопку OK.**
5. Левая часть браузера LDP отображает все дерево, которое появляется под указанным BaseDN (**OU=ldapuser, dc=wireless, dc=com**). Разверните дерево для определения местоположения пользователя **user2**. Этот пользователь может быть определен со значением CN, которое представляет имя пользователя. В данном примере это - **CN=abcd**. Дважды нажмите **CN=abcd**. В области стороны обслуживания браузера LDP **LDP отобразит все атрибуты, привязанные к user2**. Данный пример объясняет этот шаг:В данном примере наблюдайте окруженные поля справа.
6. Как упомянуто в Настраивать WLC с Подробными данными раздела Сервера LDAP этого документа, в поле **User Attribute**, вводят имя атрибута в записи пользователя, которая содержит имя пользователя.От этих выходных данных LDP вы видите, что **sAMAccountName** является одним атрибутом, который содержит имя пользователя "user2". Поэтому введите атрибут **sAMAccountName**, который соответствует полю **User Attribute** на WLC.
7. В поле **User Object Type** введите значение атрибута LDAP objectType, который определяет запись как пользователя. Часто, записи пользователя имеют несколько значений для атрибута objectType, некоторые из которых уникальны для пользователя и некоторые из которых разделены с другими типами объекта.В выходных данных LDP **КН=ПЕРСОН** является одним значением, которое определяет запись как пользователя. Поэтому задайте **Человека** как **Атрибут типа Объекта пользователя** на WLC.

Настройте беспроводного клиента

Последний шаг должен настроить беспроводного клиента для аутентификации EAP-FAST с сертификатами клиента и сервера. Выполните эти шаги для достижения этого:

1. Запустите **утилиту Cisco Aironet Desktop Utility (ADU)**. В главном окне ADU нажмите **Profile Management> New** для создания нового профиля беспроводного клиента.
2. Задайте имя профиля и назначьте название SSID к этому профилю. Это название SSID должно быть тем же, настроенным на WLC. В данном примере название SSID является **ldap**.
3. Нажмите **Вкладку Безопасность** и выберите **802.1x/EAP** в качестве безопасности уровня 2. Выберите **EAP-FAST** в качестве метода EAP и нажмите **Configure**.
4. В странице конфигурации EAP-FAST выберите **TLS Client Certificate** из раскрывающегося окна Метода аутентификации EAP-FAST и нажмите **Configure**.
5. В окне конфигурации Сертификата клиента TLS:Включите **Проверить** коробку **Установления личности Сервера** и выберите сертификат CA, установленный на клиенте (объясненный в Генерировании Корневого сертификата CA для Клиентского раздела этого документа) как Trusted Root Certification Authority.Выберите сертификат

устройства, установленный на клиенте (объясненный в Генерировании Сертификата устройства для Клиентского раздела этого документа) как сертификат клиента.**Нажмите кнопку OK.**Данный пример объясняет этот шаг:

Профиль беспроводного клиента создан.

Проверка

Выполните эти шаги, чтобы проверить, работает ли ваша конфигурация должным образом.

1. Активируйте SSID **ldap** на ADU.
2. Нажмите **Yes** или **OK** как требуется на следующих окнах. Должна существовать возможность видеть все шаги аутентификации клиента, а также ассоциации, чтобы быть успешным на ADU.

Этот раздел позволяет убедиться, что конфигурация работает правильно. Используйте режим интерфейса командой строки WLC.

- Чтобы проверить, в состоянии ли WLC связаться с Сервером LDAP и определить местоположение пользователя, задайте **команду debug aaa ldap enable** от CLI WLC. Данный пример объясняет процесс LDAP успешного обмена данными:**Примечание:** Некоторые выходные данные в этом разделе были перемещены во вторые линии, должные располагать рассмотрение с интервалами.(Cisco Controller)> **ldap debug aaa включает**
```
Sun Jan 27 09:23:46 2008: AuthenticationRequest: 0xba96514
Sun Jan 27 09:23:46 2008:       Callback.....................................0x8
344900
Sun Jan 27 09:23:46 2008:       protocolType.................................0x0
0100002
Sun Jan 27 09:23:46 2008:       proxyState...................................00:
40:96:AC:E6:57-00:00
Sun Jan 27 09:23:46 2008:       Packet contains 2 AVPs (not shown)
Sun Jan 27 09:23:46 2008: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE' (1)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to INIT
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_bind (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to CONNECTED
Sun Jan 27 09:23:46 2008: LDAP server 1 now active
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: UID Search (base=OU=ldapuser,DC=wireless, DC=com,
pattern=(&(objectclass=Person)(sAMAccountName=user2)) Sun Jan 27 09:23:46 2008:
LDAP_CLIENT: Returned msg type 0x64 Sun Jan 27 09:23:46 2008: ldapAuthRequest [1] called
lcapi_query base="OU=ldapus er,DC=wireless,DC=com" type="Person" attr="sAMAccountName"
user="user2" (rc = 0 - Success) Sun Jan 27 09:23:46 2008: LDAP ATTR> dn =
CN=abcd,OU=ldapuser,DC=Wireless,DC=com (size 38) Sun Jan 27 09:23:46 2008: Handling LDAP
response Success
```
От выделенной информации в этих выходных данных отладки ясно, что Сервер LDAP делает запрос WLC с Атрибутами пользователя, заданными на WLC, и процесс LDAP успешен.
- Чтобы проверить, успешна ли Локальная EAP-аутентификация, задайте **команду debug aaa local-auth eap method events enable** от CLI WLC. Например:(Cisco Controller)> **события метода debug aaa local-auth eap включает**
```
Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: New context
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: Allocated new EAP-FAST context
(handle = 0x22000009)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
```

(EAP handle = 0x1B000009)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Received Identity Sun Jan 27 09:38:28 2008: eap_fast_tlv.c-AUTH-EVENT: Adding PAC A-ID TLV (436973636f00000000000000000000) Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Sending Start Sun Jan 27 09:38:29 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Process Response (EAP handle = 0x1B000009) **Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Received TLS record type: Handshake in state: Start Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Local certificate found Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Hello handshake** Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: TLS_DHE_RSA_AES_128_CBC_SHA proposed... Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Proposed ciphersuite(s): Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_AES_128_CBC_SHA Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_RC4_128_SHA Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Selected ciphersuite: Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Building Provisioning Server Hello **Sun Jan 27 09:38:29 2008: eap_fast_crypto.c-EVENT: Starting Diffie Hellman phase 1 ... Sun Jan 27 09:38:30 2008: eap_fast_crypto.c-EVENT: Diffie Hellman phase 1 complete** Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: DH signature length = 128 Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: Sending Provisioning Serving Hello Sun Jan 27 09:38:30 2008: eap_fast.c-EVENT: Tx packet fragmentation required Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet(): EAP Fast NoData (0x2b) Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet(): EAP Fast NoData (0x2b) Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet(): EAP Fast NoData (0x2b) Sun Jan 27 09:38:32 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Reassembling TLS record **Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Sending EAP-FAST Ack**
.....
.....
..... **Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Received TLS record type: Handshake in state: Sent provisioning Server Hello Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Certificate handshake Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 1 to chain Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 2 to chain Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Successfully validated received certificate** Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Rx'd I-ID: "EAP-FAST I-ID" from Peer Cert Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Key Exchange handshake **Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT: Starting Diffie Hellman phase 2 ... Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT: Diffie Hellman phase 2 complete.** Sun **Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Certificate Verify handshake Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT: Sign certificate verify succeeded (compare)**
.....
.....
.....
.....
.

- Команда **debug aaa local-auth db enable** также очень полезна. Например:(Cisco Controller)> **db debug aaa local-auth включает**Sun Jan 27 09:35:32 2008: LOCAL_AUTH: EAP: Received an auth request

  Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Creating new context
  Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Local auth profile name for context 'ldapuser' Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Created new context eap session handle fb000007 Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet (id 2) to EAP subsys Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found matching context for id - 8 **Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP) Sending user credential request username 'user2' to LDAP** Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found context matching MAC address - 8
  .....
  .....
  .....
  ..... Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet (id 12) to EAP subsys

```
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8 Sun Jan 27 09:35:36
2008: LOCAL_AUTH: (EAP:8) ---> [KEY AVAIL] send_len 64, recv_len 0 Sun Jan 27 09:35:36 2008:
LOCAL_AUTH: (EAP:8) received keys waiting for success Sun Jan 27 09:35:36 2008: LOCAL_AUTH:
Found matching context for id - 8 Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Received
success event Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Processing keys success
```

- Для просмотра сертификатов, установленных в WLC, который будет использоваться для локальной проверки подлинности, выполнит **команду show local-auth certificates** от CLI WLC. Например:(Cisco Controller)**> show local-auth certificates**

```
Certificates available for Local EAP authentication:


Certificate issuer ............................. vendor

  CA certificate:

    Subject: DC=com, DC=Wireless, CN=wireless

     Issuer: DC=com, DC=Wireless, CN=wireless

      Valid: 2008 Jan 23rd, 15:50:27 GMT to 2013 Jan 23rd, 15:50:27 GMT

  Device certificate:

    Subject: O=cisco, CN=ciscowlc123

     Issuer: DC=com, DC=Wireless, CN=wireless

      Valid: 2008 Jan 24th, 12:18:31 GMT to 2010 Jan 23rd, 12:18:31 GMT


Certificate issuer ............................. cisco

  CA certificate:

    Subject: O=Cisco Systems, CN=Cisco Manufacturing CA

     Issuer: O=Cisco Systems, CN=Cisco Root CA 2048

      Valid: 2005 Jun 10th, 22:16:01 GMT to 2029 May 14th, 20:25:42 GMT

   Device certificate:

            Not installed.
```

- Для просмотра конфигурации локальной проверки подлинности на WLC от режима интерфейса командой строки выполните **команду show local-auth config**. Например:(Cisco Controller)**> show local-auth config**

```
User credentials database search order:

    Primary ..................................... LDAP


Timer:

    Active timeout ............................. 300


Configured EAP profiles:

    Name ........................................ ldapuser
```

```
      Certificate issuer ..................... vendor

      Peer verification options:

        Check against CA certificates ........... Enabled

        Verify certificate CN identity .......... Disabled

        Check certificate date validity ......... Disabled

      EAP-FAST configuration:

        Local certificate required .............. Yes

        Client certificate required ............. Yes

      Enabled methods ......................... fast

      Configured on WLANs ..................... 2


EAP Method configuration:

    EAP-FAST:

--More-- or (q)uit

      Server key ............................... <hidden>

      TTL for the PAC ......................... 10

      Anonymous provision allowed .............. No

      ........................................

      ........................................

      Authority Information .................... Cisco A-ID
```

Устранение неполадок

Можно использовать эти команды для устранения проблем конфигурации:

- **debug aaa local-auth eap method events enable**
- **debug aaa all enable**
- **пакет debug dot1x включает**

Дополнительные сведения

- Пример конфигурации проверки подлинности EAP-FAST с контроллерами беспроводной сети и внешним сервером RADIUS
- PEAP под Unified Wireless Networks с Microsoft Internet Authentication Service (IAS)
- Пример конфигурации динамического назначения VLAN с WLC на основе сопоставления групп ACS и Active Directory
- Руководство по конфигурированию контроллера Cisco Wireless LAN - решения по

обеспечению безопасности Настройки
- Руководство по конфигурированию контроллера Cisco Wireless LAN - управляющее программное обеспечение Controller и конфигурации
- Пример конфигурации аутентификации EAP в контроллерах WLAN (WLC)
- Часто задаваемые вопросы по функциям и системе контроллера беспроводной LAN (WLC)
- Cisco Secure Services Client с проверкой подлинности EAP-FAST
- Часто задаваемые вопросы по контроллеру беспроводной LAN (WLC)
- Часто задаваемые вопросы ошибок и системных сообщений контроллера беспроводной локальной сети (WLC) контроллеров
- Cisco Systems – техническая поддержка и документация