Пример конфигурации локального сервера EAP Unified Wireless Network

Содержание

Введение

В этом документе описывается конфигурация локального сервера расширяемого протокола аутентификации (EAP) в контроллере беспроводной локальной сети Cisco (WLC) для аутентификации пользователей беспроводной сети.

Локальный EAP – это способ аутентификации, который позволяет пользователям и беспроводным клиентам выполнять аутентификацию локально. 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 удаляя зависимость от внешнего сервера проверки подлинности. Локальный EAP получает учетные данные пользователя из базы локальных пользователей или базы данных бэкэнда Протокола LDAP для аутентификации пользователей. Локальный EAP поддерживает Легковесный EAP (LEAP), Гибкая аутентификация EAP через Безопасный, Туннелирующий (EAP-FAST) и Transport Layer Security EAP (EAP-TLS) аутентификация между контроллером и беспроводными клиентами.

Если существует глобальная конфигурация внешнего сервера RADIUS в WLC, Обратите внимание на то, что локальный сервер EAP не доступен. Все запросы аутентификации переданы глобальному внешнему RADIUS, пока Локальный Сервер EAP не доступен. Если WLC высвобождает подключение к внешнему серверу RADIUS, то локальный сервер EAP становится активным. Если нет никакой глобальной Конфигурации сервера RADIUS, локальный сервер EAP сразу становится активным. Локальный сервер EAP не может использоваться для аутентификации клиентов, которые связаны с другими WLC. Другими словами, один WLC не может передать свой запрос EAP к другому WLC для аутентификации. Каждый WLC должен иметь свой собственный локальный сервер EAP и отдельную базу данных.

Примечание: Используйте эти команды, чтобы мешать WLC отправить запросы к внешнему серверу RADIUS.

```
config wlan disable
        config wlan radius_server auth disable
        config wlan enable
```

Локальные поддержки сервера EAP эти протоколы в 4.1.171.0 выпусках ПО и позже:

- LEAP
- EAP-FAST (и имя пользователя/пароль и сертификаты)
- EAP-TLS

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Знание того, как настроить WLC и облегченные точки доступа (LAP) для главной операции
- Знание Протокола LWAPP и методов безопасности беспроводной связи
- Базовые знания о локальной EAP-аутентификации.

Используемые компоненты

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

- Windows XP с картой адаптера CB21AG и версией 4.05 Cisco Secure Services Client
- Контроллер беспроводной локальной сети Cisco 4400 4.1.171.0
- Microsoft Certification Authority на Сервере Windows 2000

Условные обозначения

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

Настройте локальный EAP на контроллере беспроводной

локальной сети Cisco

Этот документ предполагает, что уже завершена базовая конфигурация WLC.

Локальная конфигурация EAP

Выполните эти шаги для настройки Локального EAP:

1. Добавьте локального сетевого пользователя:От GUI. выберите **Security> Local Net Users> New**, введите Имя пользователя, Пароль, Гостя, ИДЕНТИФИКАТОР WLAN и Описание и нажмите **Apply**.От CLI можно использовать *<password>* *<username>* **config netuser add** *<идентификатор WLAN>* команда *<description>*:**Примечание:** Эта команда была переведена в нерабочее состояние к второй линии из-за пространственных причин.`(Cisco Controller) >`**`config netuser add`** *`eapuser2 cisco123 1 Employee user local database`*
2. Задайте заказ извлечения мандата пользователя.От GUI выберите **Security> Local EAP> Authentication Priority**. Затем выберите LDAP, нажмите" **<**" кнопка и нажмите **Apply**. Это помещает учетные данные пользователя в локальную базу данных сначала.От CLI:`(Cisco Controller) >`**`config local-auth user-credentials local`**
3. Добавьте EAP profile:Чтобы сделать это от GUI, выберите **Security> Local EAP> Profiles** и нажмите **New**. Когда новое окно появится, введите Имя профиля и нажмите **Apply**.Можно также сделать, это использование **config local-auth eap-profile** команды CLI **добавляет** *<profile-name>.* В нашем примере имя профиля является *тестом EAP*.`(Cisco Controller) >`**`config local-auth eap-profile add`** *`EAP-test`*
4. Добавьте метод к EAP profile.От GUI выбирают **Security> Local EAP> Profiles** и щелкают по имени профиля, для которого вы хотите добавить методы аутентификации. Данный пример использует LEAP, EAP-FAST и EAP-TLS. Нажмите **Apply** для установки методов.Можно также использовать **метод config local-auth eap-profile** команды CLI**, добавляет** *<имя метода>* *<profile-name>*. В нашем примере конфигурации мы добавляем три метода к тесту EAP профиля. Методы являются LEAP, EAP-FAST и EAP-TLS, имена методов которого являются *скачком, быстро,* и *tls* соответственно. Эти выходные данные показывают команды конфигурации интерфейса командой строки:`(Cisco Controller) >`**`config local-auth eap-profile method add leap EAP-test`** `(Cisco Controller) >`**`config local-auth eap-profile method add fast EAP-test`** `(Cisco Controller) >`**`config local-auth eap-profile method add tls EAP-test`**
5. Настройте параметры метода EAP. Это только используется для EAP-FAST. Параметры, которые будут настроены:**Серверный ключ (server-key)** — Серверный ключ для шифрования Учетных данных Защищенного доступа (PAC) (в шестнадцатеричном).**Время жизни для PAC (pac-ТТЛ-схема)** — устанавливает время жизни для PAC.**ID полномочий (идентификатор полномочий)** — Устанавливает идентификатор полномочий.**Условие Annonymous (скоро-provn)** — Настраивает, позволено ли анонимное условие. Это значение используется по умолчанию.Для конфигурации через GUI выберите **Security> Local EAP> EAP-FAST Parameters** и введите Серверный ключ, Время жизни для PAC, ID полномочий (в hex), и значения Сведений распознавания полномочий.Это команды конфигурации интерфейса командой строки для использования для установки этих параметров для EAP-FAST:`(Cisco Controller) >`**`config local-auth method fast server-key 12345678`** `(Cisco Controller) >`**`config local-auth method fast authority-id 43697369f1 CiscoA-ID`** `(Cisco Controller) >`**`config local-auth method fast pac-ttl 10`**

6. Включите локальную проверку подлинности на WLAN:От GUI выбирают **WLAN** в главном меню и выбирают WLAN, для которого вы хотите настроить локальную проверку подлинности. Новое окно появляется. Нажмите **Безопасность> вкладки AAA**. Проверьте **Локальную EAP-аутентификацию** и выберите правильное Название EAP Profile от ниспадающего меню как показано в примере:Можно также выполнить **config** CLI **wlan, локальная аутентификация включают** *<profile-name> <wlan-идентификатор>* команда настройки как показано здесь:`(Cisco Controller) >`**`config wlan local-auth enable EAP-test 1`**
7. Установите параметры безопасности уровня 2.От графического интерфейса пользователя (GUI), в Окне редактирования WLAN переходят **к Безопасности> Таблицы уровня 2** и выбрал **WPA+WPA2** из ниспадающего меню безопасности уровня 2. Под разделом Параметров WPA+WPA2, набор Шифрование WPA к **TKIP** и **AES** Шифрования WPA2. **Затем нажмите Apply.**От CLI используйте эти команды:`(Cisco Controller) >`**`config wlan security wpa enable 1`** `(Cisco Controller) >`**`config wlan security wpa wpa1 ciphers tkip enable 1`** `(Cisco Controller) >`**`config wlan security wpa wpa2 ciphers aes enable 1`**
8. Проверка конфигурации:`(Cisco Controller) >`**`show local-auth config`** `User credentials database search order: Primary ..... `**`Local DB`** `Timer: Active timeout ..... Undefined Configured EAP profiles: `**`Name ..... EAP-test`** `Certificate issuer ..... cisco Peer verification options: Check against CA certificates ..... Enabled Verify certificate CN identity ..... Disabled Check certificate date validity ..... Enabled EAP-FAST configuration: Local certificate required ..... No Client certificate required ..... No `**`Enabled methods ..... leap fast tls Configured on WLANs ..... 1`** `EAP Method configuration: EAP-FAST: --More-- or (q)uit Server key ..... <hidden> TTL for the PAC ..... 10 Anonymous provision allowed ..... Yes Authority ID ..... 43697369f10000000000000000000000 Authority Information ..... CiscoA-ID` Вы видите определенные параметры wlan 1 с командой *<wlan id>* **show wlan**:`(Cisco Controller) >`**`show wlan 1`** `WLAN Identifier..... 1 Profile Name..... austinlab Network Name (SSID)..... austinlab Status..... Disabled MAC Filtering..... Disabled Broadcast SSID..... Enabled AAA Policy Override..... Disabled Number of Active Clients..... 0 Exclusionlist Timeout..... 60 seconds Session Timeout..... 1800 seconds Interface..... management WLAN ACL..... unconfigured DHCP Server..... Default DHCP Address Assignment Required..... Disabled Quality of Service..... Silver (best effort) WMM..... Disabled CCX - AironetIe Support..... Enabled CCX - Gratuitous ProbeResponse (GPR)..... Disabled Dot11-Phone Mode (7920)..... Disabled Wired Protocol..... None --More-- or (q)uit IPv6 Support..... Disabled Radio Policy..... All `**`Local EAP Authentication..... Enabled (Profile 'EAP-test') Security`** `802.11 Authentication:..... Open System Static WEP Keys..... Disabled 802.1X..... Disabled `**`Wi-Fi Protected Access (WPA/WPA2)..... Enabled WPA (SSN IE)..... Enabled TKIP Cipher..... Enabled`** `AES Cipher..... Disabled `**`WPA2 (RSN IE)..... Enabled`** `TKIP Cipher..... Disabled `**`AES Cipher..... Enabled`** `Auth Key Management 802.1x..... Enabled PSK..... Disabled CCKM..... Disabled CKIP`

```
..................................... Disabled IP
Security.................................. Disabled IP Security
Passthru.......................... Disabled Web Based Authentication.....................
Disabled --More-- or (q)uit Web-Passthrough.............................. Disabled
Conditional Web Redirect..................... Disabled Auto
Anchor.................................... Disabled Cranite
Passthru.............................. Disabled Fortress
Passthru.............................. Disabled H-REAP Local
Switching......................... Disabled Infrastructure MFP protection.................
Enabled (Global Infrastructure MFP Disabled) Client MFP.................................
Optional Tkip MIC Countermeasure Hold-down Timer....... 60 Mobility Anchor List WLAN ID IP
Address Status
```

Существуют другие параметры локальной проверки подлинности, которые могут быть настроены, в особенности активный таймер таймаута. Этот таймер настраивает период, в течение которого используется локальный EAP после того, как все серверы RADIUS отказали.От GUI выберите **Security> Local EAP> General** и установите значение времени. **Затем нажмите Apply.**От CLI выполните эти команды:

```
(Cisco Controller) >config local-auth active-timeout ? <1 to 3600> Enter the
timeout period for the Local EAP to remain active, in seconds. (Cisco Controller) >config
local-auth active-timeout 60
```

Можно проверить значение, к которому этот таймер установлен при запуске **команды show local-auth config.**

```
(Cisco Controller) >show local-auth config User credentials database search order: Primary
..................................... Local DB Timer: Active timeout
.............................. 60 Configured EAP profiles: Name
..................................... EAP-test ... Skip
```

9. Если необходимо генерировать и загрузить ручной PAC, можно использовать или GUI или CLI.От GUI выберите **COMMANDS** из главного меню, и выбрал **Upload File** из списка в правой стороне. Выберите **PAC (Protected Access Credential)** от ниспадающего меню Типа файла. Введите все параметры и щелкните **по Upload**.От CLI введите эти команды:

```
(Cisco Controller) >transfer upload datatype pac (Cisco Controller) >transfer
upload pac ? username Enter the user (identity) of the PAC (Cisco Controller) >transfer
upload pac test1 ? <validity> Enter the PAC validity period (days) (Cisco Controller)
>transfer upload pac test1 60 ? <password> Enter a password to protect the PAC (Cisco
Controller) >transfer upload pac test1 60 cisco123 (Cisco Controller) >transfer upload
serverip 10.1.1.1 (Cisco Controller) >transfer upload filename manual.pac (Cisco
Controller) >transfer upload start Mode..................................... TFTP
TFTP Server IP.............................. 10.1.1.1 TFTP
Path..................................... / TFTP
Filename................................. manual.pac Data
Type..................................... PAC PAC
User..................................... test1 PAC
Validity................................. 60 days PAC
Password................................. cisco123 Are you sure you want to start?
(y/N) y PAC transfer starting. File transfer operation completed successfully.
```

Microsoft Certification Authority

Для использования версии 2 EAP-FAST и Проверки подлинности EAP-TLS, WLC и все устройства клиента должны иметь подтвержденный сертификат и должны также знать общий сертификат Центра сертификации.

Установка

Если Серверу Windows 2000 уже не установили сервисы Центра сертификации, необходимо установить его.

Выполните эти шаги для активации Microsoft Certification Authority на Сервере Windows 2000:

1. От Панели управления выберите **Add/Remove Programs**.:
2. Выберите **Add/Remove Windows Components** на левой части.
3. Проверьте **сервисы сертификации**.Рассмотрите это предупреждение перед переходом:
4. Выберите, какой тип Центра сертификации вы хотите установить. Для создания простых автономных полномочий выберите **Stand-alone root CA**.
5. Введите необходимую информацию о Центре сертификации. Эта информация создает подписанный сертификат для вашего Центра сертификации. Помните название CA, которое вы используете.Центр сертификации хранит сертификаты в базе данных. Данный пример использует настройку по умолчанию, предложенную Microsoft:
6. Сервисы Microsoft Certification Authority используют Сервер Веб-узла Microsoft IIS, чтобы создать и управлять сертификатами клиента и сервера. Это должно перезапустить сервис IIS для этого:Сервер Microsoft Windows 2000 теперь устанавливает новый сервис. У вас должен быть свой компакт-диск для установки Сервера Windows 2000 для установки новых окон Components.Центр сертификации теперь установлен.

Установите сертификат в контроллере беспроводной локальной сети Cisco

Для использования версии 2 EAP-FAST и EAP-TLS на локальном сервере EAP контроллера беспроводной локальной сети Cisco, выполните эти три действия:

1. Установите сертификат устройства на Контроллере беспроводной локальной сети.
2. Загрузите сертификат ЦС поставщика на контроллер беспроводной локальной сети.
3. Настройте Контроллер беспроводной локальной сети для использования EAP-TLS.

Обратите внимание на то, что в примере, показанном в этом документе, Access Control Server (ACS) установлен на том же хосте как Microsoft Active Directory и Microsoft Certification Authority, но конфигурация должна быть тем же, если сервер ACS находится на другом сервере.

Установите сертификат устройства на контроллере беспроводной локальной сети

Выполните следующие действия:

1. . Выполните эти шаги для генерации сертификата для импорта к WLC:Перейдите **к http://<serverIpAddr>/certsrv**.Выберите **Request a Certificate** и нажмите **Next**.Выберите **Advanced Request** и нажмите **Next**.Выберите **Подтверждение запроса о сертификате в данный центр сертификации с использованием формы** и нажмите **Next**.Выберите **Web-сервер** для Шаблона сертификата и введите связанные сведения. Затем отметьте ключи как **экспортные**.Вы теперь получаете сертификат, который необходимо установить в машине.
2. Выполните эти шаги для получения сертификата из ПК:Откройте браузер Internet Explorer и выберите **Tools> Internet Options> Content**.Нажмите **Certificates**.Выберите новый установленный сертификат от ниспадающего меню.Нажмите **Export**.Нажмите

Next дважды и выберите**, Yes экспортируют секретный ключ**. Этот формат является PKCS#12 (формат.PFX).Выберите **надежную защиту Enable**.Введите пароль.Сохраните его в файле <tme2.pfx>.

3. Скопируйте сертификат в формате PKCS#12 к любому компьютеру, где вам установили Openssl для преобразования его в формат PEM.`openssl pkcs12 -in tme2.pfx -out tme2.pem`
`!--- The command to be given, -in <inputfilename>.` Enter Import Password: `!--- Enter the password given previously, from step 2g.` MAC verified OK Enter PEM pass phrase: `!--- Enter a phrase.` Verifying - Enter PEM pass phrase:
4. Загрузите преобразованный сертификат устройства форматирования PEM на WLC.`(Cisco Controller) >`**`transfer download datatype eapdevcert`** `(Cisco Controller) >`**`transfer download certpassword password`** `!--- From step 3.` Setting password to <cisco123> (Cisco Controller) >**`transfer download filename tme2.pem`** (Cisco Controller) >**`transfer download start`** Mode..... TFTP Data Type..... Vendor Dev Cert TFTP Server IP..... 10.1.1.12 TFTP Packet Timeout..... 6 TFTP Max Retries..... 10 TFTP Path..... / TFTP Filename..... tme2.pem This may take some time. Are you sure you want to start? (y/N) y TFTP EAP Dev cert transfer starting. Certificate installed. Reboot the switch to use new certificate.
5. После того, как перезагруженный, проверьте сертификат.`(Cisco Controller) >`**`show local-auth certificates`** Certificates available for Local EAP authentication: Certificate issuer ..... vendor CA certificate: Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme Valid: 2007 Feb 28th, 19:35:21 GMT to 2012 Feb 28th, 19:44:44 GMT Device certificate: Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme2 Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme Valid: 2007 Mar 28th, 23:08:39 GMT to 2009 Mar 27th, 23:08:39 GMT

Загрузите сертификат ЦС поставщика на контроллер беспроводной локальной сети

Выполните следующие действия:

1. Выполните эти шаги для получения Сертификата CA Поставщика:Перейдите **к http://<serverIpAddr>/certsrv**.Выберите **Retrieve the CA Certificate** и нажмите **Next**.Выберите сертификат CA.Нажмите **закодированный DER**.Щелкните **по Download CA certificate** и сохраните сертификат как **rootca.cer**.
2. Преобразуйте Поставщика CA из формата DER в формат PEM с **openssl x509 - в rootca.cer - сообщают DER - rootca.pem-outform** команда **PEM**.Выходной файл является rootca.pem в формате PEM.
3. Загрузите сертификат ЦС поставщика:`(Cisco Controller) >`**`transfer download datatype eapcacert`** `(Cisco Controller) >`**`transfer download filename ?`** <filename> Enter filename up to 16 alphanumeric characters. (Cisco Controller) >**`transfer download filename rootca.pem`** (Cisco Controller) >**`transfer download start ?`** (Cisco Controller) >**`transfer download start`** Mode..... TFTP Data Type..... Vendor CA Cert TFTP Server IP..... 10.1.1.12 TFTP Packet Timeout..... 6 TFTP Max Retries..... 10 TFTP Path..... / TFTP Filename..... rootca.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 new certificate.

Настройте Контроллер беспроводной локальной сети для использования EAP-

TLS

Выполните следующие действия:

От GUI выберите **Security> Local EAP> Profiles**, выберите профиль и проверку для этих параметров настройки:

- Локальный Требуемый Сертификат включен.
- Требуемый Сертификат клиента включен.
- Отправитель сертификата является Поставщиком.
- Проверка против сертификатов CA включена.

Установите сертификат центра сертификации на устройстве клиента

Загрузите и установите корневой сертификат CA для клиента

Клиент должен получить корневой сертификат CA из сервера Центра сертификации. Существует несколько методов, которые можно использовать, чтобы получить сертификат клиента и установить его на машине Windows XP. Для получения подтвержденного сертификата пользователь Windows XP должен быть зарегистрирован в использовании их идентификатора пользователя и должен иметь сетевое подключение.

Web-браузер на клиенте Windows XP и проводном соединении с сетью использовался для получения сертификата клиента из частного сервера корневого центра сертификации. Эта процедура используется для получения сертификата клиента из сервера Microsoft Certification Authority:

1. Используйте web-браузер на клиенте и укажите браузер к серверу Центра сертификации. Чтобы сделать это, введите **http://IP-address-of-Root-CA/certsrv**.
2. Войдите в использование **Domain_Name\user_name**. Необходимо войти в использование имени пользователя частного лица, которое должно использовать клиента XP.
3. На Окне приветствия выберите **Retrieve a CA certificate** и нажмите **Next**.
4. Выберите **Base64 Encoding** и **Download CA certificate**.
5. На окне Certificate Issued нажмите **Install этот сертификат** и нажмите **Next**.
6. Выберите **Automatically выбирают хранилище сертификата** и **нажимают Next**, для успешного сообщения Импорта.
7. Соединитесь с Центром сертификации для получения сертификата Центра сертификации:
8. Нажмите **Download CA certificate**.
9. Чтобы проверить, что Сертификат центра сертификации правильно установлен, открытый Internet Explorer, и выберите **Tools> Internet Options> Content> Certificates**.В Trusted Root Certification Authority необходимо видеть недавно установленный Центр сертификации:

Генерируйте сертификат клиента для устройства клиента

Клиент должен получить сертификат из сервера Центра сертификации для WLC для аутентификации клиента EAP-TLS WLAN. Существует несколько методов, которые можно использовать, чтобы получить сертификат клиента и установить его на машине Windows XP. Для получения подтвержденного сертификата пользователь Windows XP должен быть зарегистрирован в использовании их идентификатора пользователя и должен иметь сетевое подключение (или проводное соединение или подключение WLAN с отключенной безопасностью 802.1x).

Web-браузер на клиенте Windows XP и проводном соединении с сетью используется для получения сертификата клиента из частного сервера корневого центра сертификации. Эта процедура используется для получения сертификата клиента из сервера Microsoft Certification Authority:

1. Используйте web-браузер на клиенте и укажите браузер к серверу Центра сертификации. Чтобы сделать это, введите **http://IP-address-of-Root-CA/certsrv**.
2. Войдите в использование **Domain_Name\user_name**. Необходимо войти в использование имени пользователя частного лица, которое использует клиента XP. (Имя пользователя встроено в сертификат клиента.)
3. На Окне приветствия выберите **Request сертификат** и нажмите **Next**.
4. Выберите **Расширенный запрос** и нажмите **Next**.
5. Выберите **Подтверждение запроса о сертификате в данный центр сертификации с использованием формы** и нажмите **Next**.
6. На Усовершенствованной Форме запроса сертификата выберите Certificate Template в качестве **Пользователя**, задайте Размер ключа как **1024** и нажмите **Submit**.
7. На окне Certificate Issued нажмите **Install этот сертификат**. Это приводит к успешной установке сертификата клиента на клиенте Windows XP.
8. Выберите **Client Authentication Certificate**.Сертификат клиента теперь создан.
9. Чтобы проверить, что сертификат установлен, перейдите к Internet Explorer и выберите **Tools> Internet Options> Content> Certificates**. Во вкладке Personal необходимо видеть сертификат.

EAP-TLS с Cisco Secure Services Client на устройстве клиента

Выполните следующие действия:

1. WLC, по умолчанию, передает SSID, таким образом, это показывают в Создать Списке сетей просмотренного SSIDs. Для создания Сетевого профиля можно нажать SSID в списке (Предприятие) и нажать **Create Network**.Если инфраструктура WLAN настроена с широковещательным отключенным SSID, необходимо вручную добавить SSID. Чтобы сделать это, **нажмите Add** под Устройствами доступа и вручную введите соответствующий SSID (например, Предприятие). **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).
2. Нажмите **Create Network** для запуска окна Network Profile, которое разрешает вам привязывать выбранный (или настроенный) SSID с механизмом аутентификации.

Назначьте описательное имя для профиля.**Примечание:** Множественные типы безопасности беспроводных сетей и/или SSIDs могут быть привязаны под этим опознавательным профилем.
3. Включите аутентификацию и проверьте метод EAP-TLS. Затем нажмите **Configure** для настройки свойств EAP-TLS.
4. В соответствии со Сводкой Конфигурации сети, нажмите **Modify** для настройки EAP / учетные параметры настройки.
5. Задайте **Включают Аутентификацию**, выбирают **EAP-TLS** в соответствии с Протоколом и выбирают **Username** в качестве Идентичности.
6. **Укажите Use Single Sign on Credentials, чтобы использовать журнал учетных данных для аутентификации сети.** Нажмите **Configure** для устанавливания параметров EAP-TLS.
7. Для имения защищенной конфигурации EAP-TLS, необходимо проверить сертификат сервера RADIUS. Чтобы сделать это, проверка **Проверяют Серверный сертификат**.
8. Для проверки сертификата сервера RADIUS необходимо дать информацию о Cisco Secure Services Client для принятия только правильного сертификата. Выберите **Client> Trusted Servers> Manage Current User Trusted Servers**.
9. Дайте название для правила и проверьте название серверного сертификата.Конфигурация EAP-TLS закончена.
10. Соединитесь с профилем Беспроводной сети. Cisco Secure Services Client просит регистрационную информацию пользователя для входа:Cisco Secure Services Client получает серверный сертификат и проверяет его (с настроенным правилом и установленный Центр сертификации). Это тогда просит сертификат использовать для пользователя.
11. **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.

Команды "debug"

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Эти команды отладки могут использоваться в WLC для мониторинга выполнения опознавательного обмена:

- **debug aaa events enable**
- **подробность debug aaa включает**
- **debug dot1x events enable**
- **состояния debug dot1x включают**
- **события debug aaa local-auth eap включают**Или

- debug aaa all enable

Дополнительные сведения

- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 4.1
- Поддержка технологии WLAN
- Cisco Systems – техническая поддержка и документация