Руководство по настройке EAP-TLS версии 1,01

ID документа: 64064

Обновлено : 14 октября 2009

Родственные продукты

- Точка доступа Cisco Aironet 1200
- Точки доступа Cisco Aironet 350
- Cisco Secure Access Control Server for Unix
- Cisco Secure Access Control Server for Windows

Содержание

Введение

Этот документ предоставляет пример конфигурации для Transport Layer Security расширяемого протокола аутентификации (EAP-TLS) Версия 1.01.

Примечание: Этот документ предполагает использование Microsoft Certificate Authority (CA). В то время как можно использовать подписанный сертификат, Cisco высоко препятствует этой практике, и этот документ не покрывает подписанные сертификаты. Период истечения по умолчанию подписанных сертификатов составляет только один год, и вы не можете изменить эти настройки. Это довольно стандартно для серверных сертификатов. Однако подписанный сертификат также действует как корневой сертификат CA. Поэтому необходимо установить новый сертификат на каждом клиенте каждый год, пока вы не проверяете опцию “Validate Server Certificate”. Real CA должен быть доступным для получения сертификатов клиента так или иначе, и таким образом, нет действительно никакой причины использовать подписанные сертификаты с EAP-TLS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Точка доступа (AP) 12.02T1
- Access Control Server (ACS) 3.1, 3. 2 и 3. 3
- Windows 2000 и XP
- Корневой центр сертификации предприятия (CA)

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.

Настройка

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

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Установите Microsoft Certificate (CA) сервер

Выполните следующие действия:

1. **Выберите Start > Settings > Control Panel.**
2. Нажмите **Add/Remove Programs** в Панели управления.
3. Выберите **Add/Remove Windows Components**.
4. Выберите Certificate Services.
5. **Нажмите кнопку Next.**
6. Нажмите **Yes** к сообщению IIS.
7. Выберите автономное (или Предприятие) узел CA.
8. **Нажмите кнопку Next.**
9. Назовите CA.**Примечание:** Все другие коробки являются дополнительными.**Примечание:** Не используйте то же название для CA как сервер ACS, потому что это может заставить клиентов PEAP отказывать аутентификацию. Корневой сертификат CA с тем же названием как серверный сертификат смущает клиентов PEAP. Эта проблема не уникальна для клиентов Cisco. Конечно, если вы не планируете использовать PEAP, это не применяется.
10. **Нажмите кнопку Next.**По умолчанию базы данных корректен.
11. **Нажмите кнопку Next.**IIS должен быть установлен перед установкой CA.

Создайте серверный сертификат

Выполните следующие действия:

1. Перейдите к CA (**http://IP_of_CA_server/certsrv/**) от вашего сервера ACS.

2. Проверьте **Запрос** коробка **сертификата**.
3. **Нажмите кнопку Next.**
4. Выберите **Расширенный запрос**.
5. **Нажмите кнопку Next.**
6. Выберите **Подтверждение запроса о сертификате в данный центр сертификации с использованием формы**.
7. **Нажмите кнопку Next.**
8. Введите имя на название (CN) коробка.
9. Установите флажок **Сертификата проверки подлинности сервера** для Намеченной Цели.**Примечание:** При использовании Предприятия CA выберите **Web Server** в первом списке.
10. Выберите эти опции под Ключевой Опцией для создания нового шаблона:**CSP — v1.0 Microsoft Base Cryptographic ProviderРазмер ключа — 1024Примечание:** Сертификаты, созданные с размером ключа, больше, чем 1024, могут работать для HTTPS, но не для PEAP.**Примечание:** Windows 2003 Enterprise CA позволяет размеры ключа, больше, чем 1024, но ключ, больше, чем 1024, не работает с PEAP. Аутентификация, может казаться, проходит в ACS, но клиент просто "зависает" в попытке аутентификации.Проверьте **Ключи Марка как экспортируемый параметрПримечание:** Microsoft изменила Шаблон веб-сервера с выпуском Windows 2003 Enterprise CA. With это изменение шаблона, вы больше не можете экспортировать ключи, и опция отображается серым. Нет никаких других шаблонов сертификата, предоставленных сервисами сертификации, которые являются для проверки подлинности сервера, или которые дают способность отметить ключи как экспортные. Для создания нового шаблона, который делает так, видит Создавание Нового раздела Шаблона сертификата.Проверьте опцию **Use Local Machine StoreПримечание:** Сохраните выборы по умолчанию для всех других опций.
11. **Нажмите кнопку Submit (Отправить).**Необходимо получить это сообщение: **Ваш запрос сертификата был получен**.

Создайте новый шаблон сертификата

Выполните следующие действия:

1. **Последовательно выберите Пуск > Выполнить.**
2. Введите **certtmpl.msc** в диалоговом окне Run и нажмите ENTER.
3. Щелкните правой кнопкой мыши **Шаблон веб-сервера** и выберите **Duplicate Template**.
4. Назовите шаблон, например, ACS.
5. Выберите вкладку **Request Handling**.
6. Проверьте **Позволять секретный ключ, чтобы быть экспортируемой** опцией.
7. Нажмите кнопку **CSP**.
8. Проверьте опцию **v1.0 Microsoft Base Cryptographic Provider**.
9. **Нажмите кнопку OK.Примечание:** Сохраните выборы по умолчанию для всех других опций.
10. **Щелкните "Применить".**
11. **Нажмите кнопку OK.**
12. Откройте моментальный снимок MMC CA - в.
13. Щелкните правой кнопкой мыши **Шаблоны сертификата** и выберите **New> Certificate Template to Issue**.

14. Выберите новый шаблон, который вы создали.
15. **Нажмите кнопку OK.**
16. Перезапустите CA.Новый шаблон включен в список Шаблона сертификата.

Иногда, когда вы пытаетесь создать новый сертификат, ошибка "`Failed to create 'CertificateAuthority.Request' object`" происходит.

Выполните эти шаги для исправления этой ошибки:

1. Выберите **Start> Administrative Tools> IIS**.
2. Разверните **веб-сайты> Веб-сайт по умолчанию**.
3. Щелкните правой кнопкой мыши **CertSrv** и выберите **Properties**.
4. Нажмите кнопку **Configuration** в разделе Прикладных режимов вкладки Virtual Directory.
5. Выберите вкладку **Options**.
6. Проверьте **Разрешать** опцию **состояния сеанса**.**Примечание:** Сохраните выборы по умолчанию для всех других опций.
7. **Дважды нажмите кнопку OK.**
8. Перезапуск IIS.**Примечание:** 2003 CA в домене 2000 года, схема которого не была подготовлена на 2003 совместимость с adprep/forestprep/domainprep, не работает с EAP. Если ваш браузер блокирует с "сообщением" `ActiveX` , необходимо выполнить исправление в этом URL: http://support.microsoft.com/default.aspx? scid=kb%3Ben-us%3B330389 .**Примечание:** Если поле CSP просто отображает "`....`", гарантируют, что у вас нет программного брандмауэра на машине, которая отправляет запрос. ZoneLabs' ZoneAlarm вызывает эту ошибку в значительной степени каждый раз. Определенное другое программное обеспечение может также вызвать эту ошибку.

Утвердите сертификат от CA

Выполните следующие действия:

1. Выберите **Start> Programs> Administrative Tools> Certificate Authority**.
2. Разверните сертификат на левой панели.
3. Выберите **Pending Requests**.
4. Щелкните правой кнопкой мыши на сертификате.
5. Выберите все задачи.
6. Выберите **Issue**.

Установите сертификат на Windows Server

Загрузите серверный сертификат к серверу ACS

Выполните следующие действия:

1. Перейдите к CA (**http://IP_of_CA_server/certsrv/**) от вашего сервера ACS.
2. Выберите **проверяют сертификат в состоянии ожидания**.
3. **Нажмите кнопку Next.**
4. Выберите сертификат.
5. **Нажмите кнопку Next.**

6. **Нажмите кнопку Install (Установить).**

Установите сертификат CA на сервере ACS

Примечание: Если ACS и CA установлены на том же сервере, эти шаги не необходимы.

1. Выполните следующие действия:

2. От вашего сервера ACS перейдите к CA (**http://IP_of_CA_server/certsrv/**).
3. Выберите **Retrieve the CA certificate или список отозванных сертификатов**.
4. **Нажмите кнопку Next.**
5. Выберите **закодированный Base 64**.
6. Нажмите **Download CA certificate**.
7. **Нажмите кнопку Open.**
8. **Нажмите кнопку Install Certificate (Установить сертификат).**
9. **Нажмите кнопку Next.**
10. Выберите **Place все сертификаты в следующем хранилище**.
11. **Нажмите кнопку Browse.**
12. Установите флажок **хранилищ Show physical**.
13. Разверните список **Доверенных корневых центров сертификации**.
14. Выберите Local Computer.
15. **Нажмите кнопку OK.**
16. **Нажмите кнопку Next.**
17. **Нажмите кнопку Finish.**Окно сообщения появляется.
18. **Нажмите кнопку OK.Примечание:** Если бы ваши сертификаты клиента были созданы через CA, отличающийся от вашего серверного сертификата, то необходимо повторить эти шаги для узла CA и любого промежуточного CAs, вовлеченного в создание сертификата клиента.

Установите ACS для Использования Серверного сертификата

Выполните следующие действия:

1. Нажмите **System Configuration** на сервере ACS.
2. Выберите **ACS Certificate Setup**.
3. Выберите **сертификат Install ACS**.
4. **Выберите вариант использования сертификата из хранилища.**
5. Введите на название CN (то же имя, которое вы ввели в Шаге 8 Создавания раздела Серверного сертификата).
6. **Нажмите кнопку Submit (Отправить).**
7. Нажмите **конфигурацию системы** на сервере ACS.
8. Выберите **ACS Certificate Setup**.
9. Выберите **Edit Certificate Trust List**.
10. Установите флажок **CA**.
11. **Нажмите кнопку Submit (Отправить).**

Создайте запрос подписи сертификата

Выполните следующие действия:

1. Перейдите **к Конфигурации системы>, Установка сертификата ACS> Генерирует Запрос подписи сертификата**.
2. Введите имя в поле Тема Сертификата в формате `cn=name`.
3. Введите имя для файла закрытого ключа.**Примечание:** Это поле кэширует путь к секретному ключу. Поэтому при нажатии **Submit** во второй раз после того, как CSR создан, секретный ключ перезаписан и не совпадет с исходным CSR. Это может привести к " , " с ошибкой, когда вы пытаетесь установить серверный сертификат.
4. Введите пароль с закрытым ключом.
5. Подтвердите пароль.
6. Выберите длину ключа 1024.**Примечание:** ACS может генерировать размеры ключа, больше, чем 1024. Однако ключ, больше, чем 1024, не работает с EAP. Аутентификация, может казаться, проходит в ACS, но клиент просто "зависает" в попытке аутентификации.
7. **Нажмите кнопку Submit (Отправить).**
8. Скопируйте выходные данные CSR на правой стороне для отправки CA.

Используйте свой CSR для создания серверного сертификата

Выполните следующие действия:

1. Перейдите к CA (**http://IP_of_CA_server/certsrv/**) от вашего сервера FTP.
2. Выберите **Request** опция **сертификата**.
3. **Нажмите кнопку Next.**
4. Выберите **Расширенный запрос**.
5. **Нажмите кнопку Next.**
6. Выберите **Submit запрос сертификата с помощью base64 кодированные PKC #10 файл или запрос на обновление с помощью base64 кодированные PKC #7 файл**.
7. Вставьте выходные данные от Шага 8 Создавания раздела Запроса подписи сертификата в поле Base64 Encoded Certificate Request.
8. **Нажмите кнопку Submit (Отправить).**
9. Нажмите **Download CA certificate**.
10. Нажмите **Save**, введите имя для сертификата и сохраните его к своему каталогу FTP.

Установите сертификат на Windows Appliance

Загрузите сертификат CA к своему Серверу FTP

Выполните следующие действия:

1. Перейдите к CA (**http://IP_of_CA_server/certsrv/**) от вашего сервера FTP.
2. Выберите **Retrieve the CA certificate или список отозванных сертификатов**.
3. **Нажмите кнопку Next.**
4. Выберите **закодированный Base 64**.
5. Нажмите **Download CA certificate**.
6. Нажмите **Save**, введите имя для сертификата и сохраните его к своему каталогу FTP.

Установите Сертификат CA на своем Устройстве

Выполните следующие действия.

1. Перейдите **к Конфигурации системы> Установка сертификата ACS> Настройка Центра сертификации ACS**.
2. Нажмите **файл Download CA certificate**.
3. Введите IP-адрес или имя хоста сервера FTP в поле FTP Server.
4. Введите допустимое имя пользователя, которое Cisco Secure ACS может использовать для доступа к серверу FTP в поле Login.
5. Введите правильный пароль для имени пользователя в Поле Password.
6. Введите относительный путь от корневого каталога сервера FTP до каталога, который содержит файл сертификата CA в поле Remote FTP Directory.
7. Введите имя файла сертификата CA в поле Remote FTP File Name.
8. **Нажмите кнопку Submit (Отправить).**
9. Проверьте имя файла в поле.
10. **Нажмите кнопку Submit (Отправить).**
11. Перезапустите сервисы ACS в **Конфигурации системы> Управление сервисами**.**Примечание:** Если вы пропускаете шаги в Сертификат CA Загрузки к вашему Сертификату CA Сервера FTP и Установки на вашей Устройстве разделах одной из этих двух ситуаций, может возникнуть:Вы не можете включить EAP-TLS, и сообщение об ошибках, кажется, сообщает, что серверный сертификат не установлен даже при том, что установлен сертификат.Также сбой `EAP type not configured` происходит в отказавшем attemtps даже при том, что настроен тип EAP.**Примечание:** Также обратите внимание, что при использовании промежуточного звена CA для создания серверного сертификата, необходимо повторить эти шаги для каждого CA в цепочке между узлом CA и серверным сертификатом (включая корневой сертификат CA). Кроме того, при создании сертификатов клиента через CA, отличающийся от серверного сертификата необходимо повторить эти шаги для узла CA и любого промежуточного CAs, вовлеченного в создание сертификата клиента.

Установите Серверный сертификат на своем Устройстве

Выполните следующие действия:

1. Перейдите **к Конфигурации системы> Установка сертификата ACS**.
2. **Нажмите кнопку Install ACS certificate (Установить сертификат ACS).**
3. Выберите сертификат Чтения от опции файла.
4. Щелкните по ссылке **файла сертификата Загрузки**.
5. Введите IP-адрес или имя хоста сервера FTP в поле FTP Server.
6. Введите допустимое имя пользователя, которое Cisco Secure ACS может использовать для доступа к серверу FTP в поле Login.
7. Введите правильный пароль в Поле Password.
8. Введите относительный путь от корневого каталога сервера FTP до каталога, который содержит файл серверного сертификата в поле Remote FTP Directory.
9. Введите имя файла серверного сертификата в поле Remote FTP File Name.
10. **Нажмите кнопку Submit (Отправить).**
11. Введите путь и пароль для секретного ключа. См. Шаги 3 и 4 Создавания раздела

Запроса подписи сертификата.

12. **Нажмите кнопку Submit (Отправить).**

Другие задачи

Настройте параметры настройки глобальной аутентификации

Выполните следующие действия:

1. Нажмите **System Configuration** на сервере ACS.
2. Нажмите **Global Authentication Setup**.
3. Проверка **позволяет EAP-TLS**.
4. Выберите одну или более опций Проверки сертификата. При выборе всех методов ACS пробует каждый метод в последовательности, пока успешная проверка не происходит или до последних сбоев метода.
5. **Нажмите кнопку Submit (Отправить).**
6. Перезапустите ПК.

Установите AP на ACS

Выполните эти шаги для устанавливания AP на ACS:

1. Нажмите **Network Configuration** на сервере ACS.
2. **Нажмите Add Запись** для добавления клиента AAA.
3. Задайте эти значения в коробках:IP-адрес клиента AAA — IP_of_your_APКлюч — Составляет ключ (удостоверьтесь, что ключ совпадает с общим секретным ключом AP),Используемая аутентификация — RADIUS (Cisco Aironet)
4. **Нажмите кнопку Submit (Отправить).**
5. Перезапустите ПК.**Примечание:** Не изменяйте ни одну из настроек по умолчанию на настройке клиента AAA.

Настройте AP

Примечание: Если вы хотите установить ACU, сетевой EAP необходим.

При использовании ротации (широковещательных) ключей вы не должны устанавливать ключ, как должен уже быть установлен ключ. Если ключ является "not set", перейдите **к Усовершенствованию> Radio Настройки** и установите значение для ротации (широковещательных) ключей. Вы, вероятно, не должны устанавливать, это немного понижает тогда 5 минут (300 secs). После установки значения **нажмите OK** и возвратитесь к странице Radio Data Encryption.

VxWorks

Выполните следующие действия:

1. Откройте AP.
2. Выберите **Setup> Security> Authentication Server**.

3. Введите IP-адрес ACS.
4. Введите общий секретный ключ. Это значение должно совпасть с ключом ACS.
5. Установите флажок **Аутентификации eap**.
6. **Нажмите кнопку OK.**
7. Выберите **Setup> Security> Radio Data Encryption**.
8. Установите **Открытый** флажок.
9. Если вы не используете ротацию (широковещательных) ключей, выберите **Ключ WEP 1** и **128**.
10. Измените Use of Data Encryption Станциями к **Полному шифрованию** (если вы не можете изменить это, нажмите **Apply** сначала).
11. **Нажмите кнопку OK.**

Веб-интерфейс AP IOS

Выполните следующие действия:

1. Выберите **Security> Server Manager**.
2. Выберите RADIUS из списка текущего сервера.
3. Введите IP-адрес ACS.
4. Введите общий секретный ключ. Это значение должно совпасть с ключом в ACS.
5. Установите флажок **Аутентификации eap**.
6. Из списка Аутентификации eap выберите IP-адрес сервера RADIUS.
7. Нажмите **OK** на диалоговом окне предупреждения.
8. **Щелкните "Применить".**

Диспетчер SSID (только шифрование WEP)

Выполните эти шаги для Шифрования WEP только:

1. Выберите SSID из Текущего Списка SSID или задайте новый SSID в поле SSID.
2. Установите флажок **Открытой аутентификации**.
3. Выберите **с EAP** из списка.
4. Установите **Сетевой** флажок **EAP**.
5. **Щелкните "Применить".**

Диспетчер шифрования (только шифрование WEP)

Выполните эти шаги для Шифрования WEP только:

1. **Выберите Security > Encryption Manager.**
2. Нажмите кнопку с зависимой фиксацией **WEP Encryption**.
3. Выберите Mandatory из списка.
4. Нажмите кнопку с зависимой фиксацией **Encryption Key 1**.
5. Задайте ключ.
6. Выберите **128** из списка Размера ключа.
7. **Щелкните "Применить".Примечание:** Конфигурация отличается при использовании WPA. Посмотрите, что управление ключами WPA добавляется в конце этого документа для подробных данных.

Загрузите и установите корневой сертификат CA для клиента

Этот шаг *требуется* для *каждого* клиента для EAP-TLS работать на того клиента. Выполните следующие действия:

1. Перейдите к CA (**http://IP_of_CA_server/certsrv/**) от клиентского компьютера.
2. Выберите **Retrieve a CA certificate**.
3. **Нажмите кнопку Next.**
4. Выберите **закодированный Base 64**.
5. Нажмите **Download CA certificate**.
6. **Нажмите кнопку Open.**
7. **Нажмите кнопку Install Certificate (Установить сертификат).**
8. **Нажмите кнопку Next.**
9. Выберите **Place все сертификаты в следующем хранилище**.
10. **Нажмите кнопку Browse.**
11. Установите флажок **хранилищ Show physical**.
12. Разверните **Доверенные корневые центры сертификации** и выберите **Local Computer**.
13. **Нажмите кнопку OK.**
14. **Нажмите кнопку Next.**
15. **Нажмите кнопку Finish.**
16. Нажмите **OK** на окне сообщения с сообщением `The import was successful.`

Создайте сертификат клиента

Предприятие CA

Выполните следующие действия:

1. Перейдите к CA (**http://IP_of_CA_server/certsrv/**) от учетной записи пользователя клиента.
2. Выберите **Request** опция **сертификата**.
3. **Нажмите кнопку Next.**
4. Выберите **Расширенный запрос**.
5. **Нажмите кнопку Next.**
6. Выберите **Подтверждение запроса о сертификате в данный центр сертификации с использованием формы**.
7. **Нажмите кнопку Next.**
8. Выберите **User** в списке Шаблона сертификата.
9. Установите эти значения под Ключевыми Опциями:CSP — v1.0 Microsoft Base Cryptographic ProviderРазмер ключа — 1024Все другие опции — Сохраняют значения по умолчанию
10. **Нажмите кнопку Submit (Отправить).**Окно сообщения появляется с сообщением `Your certificate request has been received....`

Автономный CA

Выполните следующие действия:

1. Перейдите к CA (**http://IP_of_CA_server/certsrv/**) от учетной записи пользователя клиента.
2. Выберите **Request** опция **сертификата**.
3. **Нажмите кнопку Next.**
4. Выберите **Расширенный запрос**.
5. **Нажмите кнопку Next.**
6. Выберите **Подтверждение запроса о сертификате в данный центр сертификации с использованием формы**.
7. **Нажмите кнопку Next.**
8. Введите имя пользователя в поле CN. Это значение должно совпасть с именем пользователя в базе данных проверки подлинности.
9. Выберите Client Authentication Certificate for Intended Purpose.
10. Установите эти значения под Ключевыми Опциями:CSP — v1.0 Microsoft Base Cryptographic ProviderРазмер ключа — 1024Все другие опции — Сохраняют значения по умолчанию
11. **Нажмите кнопку Submit (Отправить).**Окно сообщения появляется с сообщением `Your certificate request has been received....`

Утвердите сертификат клиента от CA

Выполните следующие действия:

1. Выберите **Start> Programs> Administrative Tools> Certificate Authority** для открытия CA.
2. Разверните сертификат слева.
3. Нажмите **Pending Requests**.
4. Щелкните правой кнопкой мыши на сертификате и выберите все задачи.
5. Выберите **Issue**.

Установите сертификат клиента на клиентском компьютере

Выполните следующие действия:

1. Перейдите к CA (**http://IP_of_CA_server/certsrv/**) от учетной записи пользователя клиента.
2. Выберите **проверяют сертификат в состоянии ожидания**.
3. **Нажмите кнопку Next.**
4. Выберите сертификат.
5. **Нажмите кнопку Next.**
6. **Нажмите кнопку Install (Установить).Примечание:** Для проверки установки сертификатов перейдите к Microsoft Internet Explorer и выберите **Tools> Internet Options> Content> Certificates**. Сертификат с названием ID вошедшия в систему пользователь или имени пользователя должен присутствовать.

Доверяйте сертификату клиента на ACS

Необходимо выполнить эти шаги, только если сертификаты клиента и серверный сертификат были созданы через другой CAs.

1. Гарантируйте, что корневой сертификат CA и Промежуточные сертификаты CA были установлены согласно шагам в Установку Сертификат CA на Сертификате CA Сервера ACS и Установки на ваших разделах Устройства.
2. Перейдите **к Конфигурации системы> Установка сертификата ACS** на ACS.
3. **Щелкните Edit Certificate Trust List (Редактировать список доверенных сертификатов).**
4. Установите флажок рядом с узлом CA, который создал сертификат клиента.
5. **Нажмите кнопку Submit (Отправить).**

Установите клиента для EAP-TLS

Выполните следующие действия:

1. **Выбрать Start> Control Panel> Network Connections**.
2. Щелкните правой кнопкой мыши беспроводную сеть и выберите **Properties**.
3. Нажмите вкладку **Wireless Network**.
4. Гарантируйте, что**...** проверены **окна использования для настройки**.
5. Нажмите **Configure**, если вы видите SSID в списке. В противном случае **нажмите Add**.
6. Вставьте SSID.
7. Проверьте **WEP**, и **Ключ предоставлен для меня автоматически** флажки.
8. Выберите **вкладку Authentication**.**Примечание:** Если вы не видите вкладку Authentication, сервис 802.1X установлен в отключенном состоянии. Для решения этой проблемы необходимо включить сервис Конфигурации беспроводной сети в списке сервисов. Выполните следующие действия:Щелкните правой кнопкой мыши **Мой компьютер** и выберите **Manage**.Нажмите **Services и Applications**.**Нажмите кнопку Services (Службы).**Установите значение Запуска для сервиса к **Автоматическому**.Запустите этот сервис.**Примечание:** Если вкладка Authentication присутствует, но недоступна, это указывает, что драйвер сетевого адаптера не поддерживает 802.1x правильно. См. Использование аутентификации 802.1x на компьютерах клиента, которые выполняют Windows 2000 .
9. Гарантируйте, что **включают контроль за сетевым доступом, использующий...** проверен.
10. Выберите **Smart Card или** тип **Other Certificate for EAP**, и нажмите **Properties**.
11. Выберите **сертификат Использования на этом параметре компьютера**.
12. Проверьте флажок **выбора простого сертификата Использования**.
13. Установите флажок для CA под Сертификатом доверенного корня.
14. Нажмите **OK** трижды.

Дополнение аутентификации компьютера

Аутентификация компьютера EAP-TLS *требует* и Active Directory и узла CA Предприятия. Для получения сертификата за аутентификацию компьютера EAP-TLS компьютер должен иметь подключение к Предприятию CA или посредством проводного соединения или посредством беспроводного соединения с отключенной безопасностью 802.1x. Это - *единственный* способ получить допустимый сертификат компьютера (с “Машиной” в поле “Certificate Template”). Когда завершено, сертификат компьютера установлен в папке **Certificates (Local Computer)> Personal> Certificates**, когда просматривается в Сертификатах (Локальный компьютер) моментальный снимок MMC - в. Сертификат содержит полностью определенное AD имя машины в полях Subject и SAN. Сертификат, который носит имя

компьютера, но не был создан, как описано в этом разделе, *не* является истинным сертификатом компьютера (с “Машиной” в поле Certificate Template). Такой сертификат не используется для аутентификации компьютера, а скорее ОС рассматривает такой сертификат как сертификат обычного пользователя.

ACS настройки для разрешения аутентификации компьютера

Выполните следующие действия:

1. Перейдите **к Внешним базам данных пользователей> Конфигурация базы данных**.
2. **Выберите Windows Database (База данных Windows).**
3. **Нажмите кнопку Configure (Настроить).**
4. Проверьте **Разрешать** флажок **аутентификации компьютера EAP-TLS**.
5. **Нажмите кнопку Submit (Отправить).**

Настройте домен для автоматической подачи заявок сертификата

Выполните следующие действия:

1. Откройте Пользовательский и Компьютерный моментальный снимок MMC - в на контроллере домена.
2. Щелкните правой кнопкой мыши запись домена и выберите **Properties**.
3. Перейдите к вкладке **Group Policy**.
4. выберите **Default Domain Policy**.
5. **Нажмите Edit.**
6. Перейдите **к Computer Configuration> Windows Settings> Security Settings> Политика С открытым ключом**.
7. Щелкните правой кнопкой мыши **автоматические параметры настройки запроса сертификата**.
8. Выберите **New> Automatic Certificate Request**.
9. **Нажмите кнопку Next.**
10. Выделите **компьютер**.
11. **Нажмите кнопку Next.**
12. Проверьте CA. предприятия
13. **Нажмите кнопку Next.**
14. **Нажмите кнопку Finish.**

Установите Client for Machine Authentification

Подключитесь к домену

Если бы клиент присоединился к домену перед настройкой автоматической подачи заявок то сертификат должен быть выполнен к машине в следующий раз, когда вы перезагружаете компьютер после того, как автоматическая подача заявок настроена без потребности воссоединиться с компьютером к домену.

Выполните эти шаги для присоединения к домену:

1. Войдите в Windows с учетной записью, которая имеет администраторские привилегии.
2. Щелкните правой кнопкой мыши на **Моем компьютере** и выберите **Properties**.
3. Выберите вкладку **Computer Name**.
4. **Нажмите кнопку «Изменить».**
5. Введите имя хоста в Поле Имя компьютера.
6. Выберите **Domain**.
7. Введите имя домена.
8. **Нажмите кнопку ОК.**Диалоговое окно входа в систему появляется.
9. Войдите с учетными данными учетной записи, которая имеет разрешения для присоединения к домену.Компьютер присоединяется к домену.
10. Перезапустите компьютер.Компьютер является теперь участником домена и имеет сертификат для CA и установленного сертификата компьютера.

Соискатель EAP-TLS настройки для аутентификации компьютера

Выполните следующие действия:

1. **Выбрать Start> Control Panel> Network Connections**.
2. Щелкните правой кнопкой мыши сетевое подключение и выберите **Properties**.
3. Выберите **вкладку Authentication**.
4. Проверка **Аутентифицируется как компьютер**.

Дополнение управления ключами WPA

Этот раздел применим к Cisco IOS AP 12.02 (13) JA1, ACS 3.2 и SP1 XP с исправлением WPA. Согласно документации в этом разделе, клиенты Windows 2000 исходно не поддерживают управление ключами WPA, и необходимо использовать клиентское программное обеспечение поставщика для получения этой поддержки. См. Обзор WPA безопасность беспроводной связи обновляют в Windows XP .

Cisco ACU не поддерживает управление ключами WPA для основанного на хосте EAP (EAP-TLS и PEAP) в настоящее время. Необходимо установить стороннего клиента, например, фанкового Клиента Odyssey или Клиента aegis Meetinghouse. См. Документы Адаптера беспроводной сети для Windows для получения дополнительной информации о WPA поддерживают для продуктов Cisco. Эта информация применима к Windows Mobile 2003 (карманных ПК) клиента также.

Управление ключами WPA является в основном тем же, но отличается по этим двум процедурам:

1. Настройте AP.
2. Установите Клиента XP для EAP-TLS и WPA.

Настройте AP

Выполните следующие действия:

1. Перейдите **к Безопасности> Диспетчер шифрования**.
2. Нажмите **Параметр WEP Cipher**.

3. Выберите **TKIP**.
4. **Щелкните "Применить".**
5. Перейдите **к Безопасности> Диспетчер SSID**.
6. Выберите SSID из Текущего Списка SSID. Также можно задать новый SSID в поле SSID.
7. Проверьте **открытую аутентификацию**.
8. Выберите **с EAP** из списка.
9. Проверьте **сетевой EAP**.
10. Выберите **Mandatory** из списка под Аутентифицируемым Управлением ключами.
11. Нажмите **WPA**.
12. **Щелкните "Применить".**

Установите Клиента XP для EAP-TLS и WPA

Выполните следующие действия:

1. **Выбрать Start> Control Panel> Network Connections**.
2. Щелкните правой кнопкой мыши беспроводную сеть и выберите **Properties**.
3. Выберите вкладку **Wireless Network**.
4. Гарантируйте, что проверены **окна использования к опции configure**.
5. Нажмите **Configure**, если вы видите SSID в списке. В противном случае **нажмите Add**.
6. Вставьте SSID.
7. Выберите **WPA for Network Authentication**.
8. Выберите **TKIP for Data Encryption**.
9. Выберите **вкладку Authentication**.
10. Гарантируйте, что **включают использование контроля за сетевым доступом**, проверен.
11. Выберите тип **Other Certificate for EAP или Smart Card**.
12. **Нажмите Properties.**
13. Выберите **сертификат Использования на этом параметре компьютера**.
14. Проверьте флажок **выбора простого сертификата Использования**.
15. Установите флажок для CA под Сертификатом доверенного корня.
16. Нажмите **OK** трижды.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Ошибка: Проблема с Сертификатом при соединении с WLAN

Эта ошибка появляется на беспроводном клиенте.

```
The server "<Authentication server>" presented a valid certificate issued by "<CA name>", but
"<CA name>" is not configured as a valid trust anchor for this profile.
```

Решение

Для решения этого вопроса можно экспортировать корневой сертификат CA, который выполнил сертификат к серверу проверки подлинности к файлу. Скопируйте файл беспроводному клиенту и затем выполните эту команду от поднятой Командной строки.

```
certutil -enterprise -addstore NTAuth CA_CertFilename.cer
```

См. сигнал безопасности Windows появляется при соединении с беспроводной сетью на машине рабочей группы для получения дополнительной информации.

Дополнительные сведения

- Страница поддержки Cisco Secure ACS для Windows
- Страница поддержки Cisco Secure ACS для UNIX
- Cisco Systems – техническая поддержка и документация

Соответствующие дискуссии сообщества технической поддержки Cisco

Сообщество технической поддержки Cisco является форумом, в котором можно задавать вопросы и получать ответы, обмениваться предложениями и сотрудничать со своими равноправными коллегами.

Обновлено : 14 октября 2009
ID документа: 64064