Установка сертификата на программно-аппаратном комплексе Cisco Secure ACS для клиентов PEAP

Содержание

Введение

В этом руководстве описываются сертификаты, создаваемые посредством Microsoft CA, а также приводится порядок действий при использовании самостоятельно подписанного сертификата, который поддерживается в Cisco Secure Access Control Server (ACS) 3.3. Использование самостоятельно подписанного сертификата значительно упрощает начальную настройку защищенного расширяемого протокола аутентификации (PEAP) благодаря исключению необходимости во внешнем центре сертификации. Однако в настоящее время срок действия самостоятельно подписанного сертификата по умолчанию составляет только один год и не может быть изменен. Это стандартная практика для серверных сертификатов. Однако, потому что подписанный сертификат также действует как корневой сертификат CA, это может означать установку нового сертификата на каждом клиенте каждый год при использовании Microsoft supplicant, пока вы не проверяете опцию **Validate Server Certificate**. Cisco рекомендует использовать самостоятельно подписанные сертификаты только как временную меру при возможности использования традиционного центра сертификации. Если вы хотите использовать самостоятельно подписанный сертификат, перейдите к разделу о самостоятельно подписанных сертификатах.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Cisco IOS® Access Point (AP) 12.02T1
- Cisco Secure ACS для Windows 3.1 и позже
- Прикладное устройство управления услугами Solution Engine (SE) Cisco Secure ACS.
- Microsoft Windows 2000 (SP3 и SP4) или XP с версией ACU 6 (при использовании Cisco Secure ACS 3.2 ACU не требуется),

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.

Microsoft Certificate Service Installation

Выполните следующие действия:

1. **Выберите Start > Settings > Control Panel.**
2. В Панели управления откройте **Добавления/удаления программы.**
3. В Добавлениях/удалениях программы выберите **Add/Remove Windows Components**.
4. Проверьте **Сервисы сертификации** и нажмите **Next**. Нажмите **да** к сообщению IIS.
5. Выберите Stand-alone (или Enterprise) узел CA и нажмите **Next**.
6. Дайте CA название и нажмите **Next**. Все другие коробки являются дополнительными.**Примечание:** Не давайте CA то же название как сервер Cisco Secure ACS. Это может заставить клиентов PEAP отказывать аутентификацию, потому что они запутываются, когда корневой сертификат CA найден с тем же названием как серверный сертификат. Эта проблема не уникальна для клиентов Cisco.
7. **Нажмите кнопку Next.**
8. **Нажмите кнопку Finish.Примечание:** Необходимо установить IIS перед установкой CA.

Cisco Secure ACS для настройки сертификата окна

Шаг 1: Создайте серверный сертификат

Выполните эти шаги для создания серверного сертификата.

1. От вашего сервера Cisco Secure ACS перейдите к CA **http://IP_of_CA_server/certsrv/**.
2. Выберите **Request** опция **сертификата** и нажмите **Next**.
3. Выберите **Расширенный запрос** и нажмите **Next**.
4. Выберите **Подтверждение запроса о сертификате в данный центр сертификации с использованием формы** и нажмите **Next**.
5. Введите что-то на название (CN) коробка.
6. Выберите **Server Authentication Certificate for Intended Purpose**.**Примечание:** Выберите **Web Server** на первом раскрывающемся окне при использовании CA. Предприятия**CSP** — v1.0 Microsoft Base Cryptographic Provider**Размер ключа** — 1024 **Примечание:** Windows 2003 Enterprise CA позволяет размеры ключа, больше, чем 1024. Однако использование ключа, больше, чем 1024, не работает с PEAP. Аутентификация, могло бы казаться, прошла бы в ACS, но клиент просто "зависает", в то время как это делает попытку аутентификации.Ключи метки выбора как экспортные.Проверьте **Память локального компьютера Использования** (только ACS программного обеспечения).Оставьте все остальное как по умолчанию и нажмите **Submit**.Сообщение появляется, который сообщает `Your certificate request has been received...`.**Примечание:** Сертификаты, созданные с размером ключа, больше, чем 1024, не работают.

Примечание 2

Примечание: Microsoft изменила Шаблон веб-сервера с выпуском Windows 2003 Enterprise CA так, чтобы ключи больше не были экспортными, и опция отображается серым. Нет никаких других шаблонов сертификата, предоставленных сервисами сертификации, которые являются для проверки подлинности сервера и дают способность отметить ключи как экспортные, которые доступны в выпадающем. Поэтому необходимо создать новый шаблон, который делает так.

Выполните следующие действия:

1. Выберите **Start> Run> certtmpl.msc**.
2. Щелкните правой кнопкой мыши **Шаблон веб-сервера** и выберите **Duplicate Template**.
3. Назовите шаблон с названием, которое легко определить.
4. Перейдите к вкладке Request Handling, и проверка **Позволяют секретному ключу экспортироваться**.
5. Щелкните по кнопке **CSP** и проверьте **v1.0 Microsoft Base Cryptographic Provider**. **Нажмите кнопку OK.**
6. Все другие опции можно оставить в по умолчанию.
7. Нажмите **Apply** и **OK**.
8. Откройте моментальный снимок MMC CA - в.
9. Щелкните правой кнопкой мыши **Шаблоны сертификата** и выберите **New> Certificate Template to Issue**.
10. Выберите новый шаблон, который вы создали, и нажмите **OK**.
11. Перезапустите CA.

Когда попытка предпринята для создания нового сертификата, сервисы сертификации могут также дать ошибку `Failed to create 'CertificateAuthority.Request' object`. Выполните эти шаги для исправления этой проблемы:

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. Перейдите к вкладке Options, и проверка **Включают состояние сеанса**.
6. Все остальное может быть оставлено в покое.
7. **Дважды нажмите кнопку OK.**
8. Перезапуск IIS.Если ваши блокировки браузера с сообщением `Downloading ActiveX Control`, работайте, исправление, обсужденное в Internet Explorer документа Microsoft, Прекращает Отвечать при "Загрузке элемента управления ActiveX" сообщение Когда Вы Попытка Использовать Сервер сертификатов. Если поле CSP только сообщает `Loading...`, удостоверьтесь, что вы не выполняете программный брандмауэр на машине, которая отправляет запрос.

Шаг 2: Утвердите сертификат от CA

Выполните следующие действия:

1. Откройте CA и **chooseStart> Программы> Средства администрирования> Центр сертификации**.

2. Слева, разверните сертификат, затем нажмите **Pending Requests**.
3. Щелкните правой кнопкой мыши на сертификате, выберите **все задачи** и выберите **Issue**.

Шаг 3: Загрузите серверный сертификат к серверу Cisco Secure ACS

Выполните следующие действия:

1. От вашего сервера Cisco Secure ACS перейдите к **CA-http://**каталог **IP_of_CA_server/certsrv/**.
2. Выберите **проверяют Сертификат В состоянии ожидания** и нажимают **Next**.
3. Выберите сертификат и нажмите **Next**.
4. **Нажмите кнопку Install (Установить).**

Шаг 4. : Установите сертификат CA на сервере Cisco Secure ACS

Выполните следующие действия:

Примечание: Если Cisco Secure ACS и CA установлены на том же сервере, этот шаг не требуется.

1. От вашего сервера Cisco Secure ACS перейдите к **CA-http://**каталог **IP_of_CA_server/certsrv/**.
2. Выберите **Retrieve the CA certificate или список отозванных сертификатов** и нажмите **Next**.
3. Выберите **Base 64 encodedand** нажимают **Download CA certificate**.
4. Нажмите **Open** и выберите **сертификат Install**.
5. **Нажмите кнопку Next.**
6. Выберите **Place все сертификаты в следующем хранилище** и нажмите **Browse**.
7. Установите флажок **хранилищ Show physical**.
8. Разверните **Доверенные корневые центры сертификации**, выберите **Local Computer** и нажмите **OK**.
9. **Нажмите Next**, **Конец**, и нажмите**, OK** для **импорта был успешной** коробкой.

Шаг 5. : Установите Cisco Secure ACS для использования Серверного сертификата

Выполните следующие действия:

1. На сервере Cisco Secure ACS нажмите **System Configuration**.
2. Выберите **сертификат Install ACS** и **ACS Certificate Setup**.
3. Выберите **сертификат Use из хранилища**.
4. Введите в CN, называют и нажимают **Submit**.
5. На сервере Cisco Secure ACS нажмите **System Configuration**.
6. Выберите **ACS Certificate Setup** и **Edit Certificate Trust List**.
7. Установите флажок для CA и нажмите **Submit**.

Настройка сертификата устройства Cisco Secure ACS

Шаг 1: Создайте запрос подписи сертификата

Выполните следующие действия:

1. Выберите **System Configuration> ACS Certificate Setup> Generate Certificate Signing Request**.
2. Введите имя в поле Тема Сертификата с форматом `cn=name`.
3. Введите имя для файла закрытого ключа.**Примечание:** Путь к секретному ключу кэшируется в этом поле. Если вы нажимаете**, подвергаются** во второй раз после того, как CSR создан, секретный ключ перезаписан и не совпадает с исходным CSR. Когда вы пытаетесь установить серверный сертификат, этот результат в с сообщением об ошибках.
4. Введите пароль с закрытым ключом и подтвердите его.
5. Выберите длину ключа 1024.**Примечание:** В то время как Cisco Secure ACS может генерировать размеры ключа, больше, чем 1024, использование ключа, больше, чем 1024, не работает с PEAP. Аутентификация, могло бы казаться, прошла бы в Cisco Secure ACS, но клиент "зависает", в то время как предпринята аутентификация.
6. **Нажмите кнопку Submit (Отправить)**
7. Скопируйте выходные данные CSR на правой стороне для подчиненного к CA.

Шаг 2: Создайте Серверный сертификат со своим CSR

Выполните следующие действия.

1. От вашего сервера FTP перейдите к **CA-http://**каталог **IP_of_CA_server/certsrv/**.
2. Выберите **Request** опция **сертификата** и нажмите **Next**.
3. Выберите **Advanced Request** и нажмите **Next**.
4. Выберите **Submit запрос сертификата с помощью base64 кодированные PKC #10 файл или запрос на обновление с помощью base64 кодированные PKC #7 файл**.
5. Вставьте выходные данные от Запроса подписи сертификата в поле Base64 Encoded Certificate Request и нажмите **Submit**.
6. Нажмите **Download CA certificate**.
7. Нажмите **Save**, назовите сертификат и сохраните его к вашему каталогу FTP.

Шаг 3: Загрузите сертификат CA к своему Серверу FTP

Выполните следующие действия:

Примечание: При пропуске этих шагов это приводит к любой неспособности включить PEAP. Вы также получаете ошибку, что серверный сертификат не установлен даже при том, что это, или вы получаете EAP сбой в неудачных попытках даже при том, что настроен тип EAP.

Примечание: Также обратите внимание, что, если ваш серверный сертификат создан с помощью промежуточного звена CA, необходимо повторить эти шаги для каждого CA в цепочке между узлом CA и серверным сертификатом, который включает корневой сертификат CA.

1. От вашего сервера FTP перейдите к **CA-http://**каталог **IP_of_CA_server/certsrv/**.

2. Выберите **Retrieve the CA certificate или список отозванных сертификатов** и нажмите **Next**.
3. Выберите **закодированный Base 64** и нажмите **Download CA certificate**.
4. Нажмите **Save** и назовите сертификат. Сохраните его к своему каталогу FTP.

Шаг 4. : Установите Сертификат CA на своем Устройстве

Выполните следующие действия:

Примечание: При пропуске этих шагов это приводит к любой неспособности включить PEAP. Вы также получаете ошибку, что серверный сертификат не установлен даже при том, что это, или вы получаете EAP сбой в неудачных попытках даже при том, что настроен тип EAP.

Примечание: Также обратите внимание, что, если ваш серверный сертификат создан с помощью промежуточного звена CA, необходимо повторить эти шаги для каждого CA в цепочке между узлом CA и серверным сертификатом, который включает корневой сертификат CA.

1. Выберите **System Configuration> ACS Certificate Setup> ACS Certification Authority Setup**.
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 пароль 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 и нажмите **Submit**.
10. Перезапустите сервисы ACS в **Конфигурации системы> Управление сервисами**.

Шаг 5. : Установите Серверный сертификат на своем Устройстве

Выполните следующие действия:

1. Выберите **System Configuration> ACS Certificate Setup**.
2. **Нажмите кнопку Install ACS certificate (Установить сертификат ACS).**
3. Выберите **сертификат Чтения** из опции файла и затем щелкните по ссылке **файла сертификата Загрузки**.
4. Введите IP-адрес или имя хоста сервера FTP в поле FTP Server.
5. Введите допустимое имя пользователя, которое Cisco Secure ACS может использовать для доступа к серверу FTP в поле Login.
6. Введите пароль пользователя в Поле Password.
7. Введите относительный путь от корневого каталога сервера FTP до каталога, который содержит файл серверного сертификата в поле Remote FTP Directory.
8. Введите имя файла серверного сертификата в поле Remote FTP File Name.
9. **Нажмите кнопку Submit (Отправить).**
10. Введите путь к секретному ключу.

11. Введите пароль для секретного ключа.
12. **Нажмите кнопку Submit (Отправить).**

Настройка Подписанного сертификата (только если вы не используете внешний CA),

Примечание: Когда вы тестируете в лабораторной работе с подписанными сертификатами, она заканчивается в более длинное опознавательное время первоначально, клиент аутентифицируется с Microsoft supplicant. Все последующие аутентификации прекрасны.

Выполните следующие действия:

1. На сервере Cisco Secure ACS нажмите **System Configuration**.
2. Нажмите **ACS Certificate Setup**.
3. Нажмите **Generate Self-signed Certificate**.
4. Введите что-то в поле Тема Сертификата, которому предшествует **cn =**, например, cn=ACS33.
5. Введите полный путь и название сертификата, который вы хотите создать, например, c:\acscert \acs33.cer.
6. Введите полный путь и название файла закрытого ключа, который вы хотите создать, например, c:\acscert \acs33.pvk.
7. Введите и подтвердите пароль с закрытым ключом.
8. Выберите **1024** из раскрывающегося меню длины ключа.**Примечание:** В то время как Cisco Secure ACS может генерировать размеры ключа, больше, чем 1024, использование ключа, больше, чем 1024, не работает с PEAP. Аутентификация, могло бы казаться, прошла бы в ACS, но клиент "зависает", в то время как предпринята аутентификация.
9. Проверьте**, что Установка генерировала сертификат**.
10. **Нажмите кнопку Submit (Отправить).**

Настройте параметры настройки глобальной аутентификации

Выполните следующие действия.

1. На сервере Cisco Secure ACS нажмите **System Configuration**.
2. Нажмите **Global Authentication Setup**.**Для версии 3.2 Cisco Secure ACS и позже**Проверка **Позволяет EAP-MSCHAPv2** при использовании Microsoft PEAP.Проверка **Позволяет EAP-GTC** при использовании PEAP Cisco.Проверка **позволяет аутентификацию версии MS-CHAP 1**.Проверка **позволяет аутентификацию версии MS-CHAP 2**.Нажмите **Submit** и **Restart**.**Для версии 3.1 Cisco Secure ACS**Проверка **позволяет PEAP**.Проверка **позволяет аутентификацию версии MS-CHAP 1**.Проверка **позволяет аутентификацию версии MS-CHAP 2**.Нажмите **Submit** и **Restart**.

Установите AP на Cisco Secure ACS

Выполните следующие действия:

1. На сервере Cisco Secure ACS нажмите **Network Configuration**.
2. **Нажмите Add Запись** для добавления клиента AAA.
3. Заполните эти коробки:**IP-адрес клиента AAA** — IP_of_your_AP**Ключ** — Составляет ключ и удостоверяется, что это совпадает на общем секретном ключе AP.**Используемая аутентификация** — RADIUS (Cisco Aironet)
4. Нажмите **Submit** и **Restart**.**Примечание:** Ни одна из настроек по умолчанию на настройке клиента AAA не была изменена.

Настройте AP

С VxWorks

Выполните следующие действия:

1. Откройте AP и выберите **Setup> Security> Authentication Server**.Введите IP-адрес Cisco Secure ACS.Введите общий секретный ключ, который должен совпасть с Ключом в Cisco Secure ACS.Проверьте **аутентификацию eap**.**Нажмите кнопку OK.**
2. Выберите **Setup> Security> Radio Data Encryption**.Проверьте **открытый**, и **Network-EAP** для принимают тип проверки подлинности.Проверьте **открытый** для, требуют EAP.Если вы не используете ротацию (широковещательных) ключей, **ключ WEP** набора **1** и выбирает **128 битов**.Use of Data Encryption изменения Станциями к **полному шифрованию**. Если вы не можете изменить use of data encryption, нажмите **Apply** сначала.**Нажмите кнопку OK.**

С веб-интерфейсом AP Cisco IOS

Выполните следующие действия:

1. Откройте AP и выберите **Security> Server Manager**.Выберите **RADIUS** из Списка Текущего сервера выпадают.Введите IP-адрес Cisco Secure ACS.Введите общий секретный ключ, который должен совпасть с 'КЛЮЧЕВЫМ' в Cisco Secure ACS.Проверьте **аутентификацию eap**.Нажмите **OK** на диалоге предупреждения и затем нажмите **Apply**.
2. **Выберите Security > SSID Manager.Примечание:** Конфигурация отличается при использовании WPA. Посмотрите, что управление ключами WPA добавляется в конце этого документа для подробных данных.Выберите SSID из Текущего Списка SSID или введите новый SSID в поле SSID.Проверьте **Открытую аутентификацию** и выберите **с EAP** из раскрывающегося меню.Проверьте **сетевой EAP**.Оставьте все другие значения в их настройках по умолчанию и нажмите **Apply**.
3. **Выберите Security > Encryption Manager.Примечание:** Конфигурация отличается при использовании WPA. Посмотрите, что управление ключами WPA добавляется в конце этого документа для подробных данных.Нажмите кнопку с зависимой фиксацией **WEP Encryption** и выберите **Mandatory** из выпадающего.Нажмите кнопку с зависимой фиксацией **Encryption Key 1** и введите ключ в поле.Выберите **128 битов** от Размера ключа выпадают.**Щелкните "Применить".**

Примечание: Сеть EAP требуется при установке ACU.

Примечание: При использовании ротации (широковещательных) ключей вы не должны

устанавливать ключ, так как должен уже быть установлен ключ. Если ключ является "not set", выберите **Усовершенствование> Radio Setup** и установите значение для ротации (широковещательных) ключей. Нет никакой потребности установить, это немного понижает тогда пять минут (300 секунд). Как только значение установлено, нажмите **OK** и возвратитесь в страницу Radio Data Encryption.

Установите Версию ACU 6 (только если вы используете Cisco Secure ACS 3.1 или если вы требуете EAP-GTC),

Необходимо выбрать Заказную установку, потому что инициатор запроса PEAP Cisco не установлен быстрой установкой. Можно сказать, установлен ли соискатель Cisco, когда вы посмотрели на тип EAP во вкладке Authentication ваших свойств сетевого подключения. Если это обнаруживается как PEAP, это - соискатель Microsoft PEAP. Если это обнаруживается как просто PEAP, то вы используете инициатор запроса PEAP Cisco.

Установите корневой сертификат CA для клиента (только для EAP-MSCHAP-V2)

При использовании сертификат от Microsoft CA

Выполните следующие действия:

1. От клиентского компьютера перейдите к CA-**http://IP_of_CA_server/certsrv/**.
2. Выберите **Retrieve a CA certificate** и нажмите **Next**.
3. Выберите **Base64 Encoding** и **Download CA certificate**.
4. Нажмите **Open** и выберите **Install Certificate**.
5. **Нажмите кнопку Next.**
6. Выберите **Place все сертификаты в следующем хранилище** и затем нажмите **Browse**.
7. Установите флажок **хранилищ Show physical**.
8. Разверните **Доверенные корневые центры сертификации**, выберите локальный компьютер и нажмите **OK**.
9. **Нажмите Next**, нажмите **Finish** и нажмите**, OK** для **импорта был успешной** коробкой.

При использовании Подписанный сертификат от Cisco Secure ACS

Выполните следующие действия:

1. Скопируйте сертификат от его местоположения до клиента.
2. **Нажмите правой кнопкой на учетной записи.** файл **cer** и щелчок **устанавливают сертификат**.
3. **Нажмите кнопку Next.**
4. Выберите **Place все сертификаты в следующем хранилище** и нажмите **Browse**.
5. Проверьте **хранилища show physical**.
6. Разверните **Доверенные корневые центры сертификации**, выберите **Local Computer** и нажмите **OK**.
7. **Нажмите Next**, нажмите **Finish** и нажмите **OK**.**Примечание:** Установите AP для Cisco Secure ACS, требуется для каждого клиента, если вы используете EAP-MSCHAP-V и имеете **Проверить** коробку **серверного сертификата**, зарегистрировался в свойствах

PEAP Windows.

Установите Клиента для PEAP

Установите Windows XP SP1 или SP для PEAP

Выполните следующие действия:

Примечание: Эта конфигурация отличается при использовании WPA. Посмотрите раздел управления ключами WPA этого документа для подробных данных.

Примечание: Windows XP SP2 в настоящее время имеет проблемы с аутентификацией PEAP к серверам RADIUS кроме IAS. Это задокументировано в KB885453, и Microsoft имеет исправление в наличии после запроса.

1. Соединения Открытой сети на панели управления и выбирают **Start> Control Panel**).
2. Щелкните правой кнопкой мыши беспроводную сеть и выберите **Properties**.
3. На вкладке беспроводной сети удостоверьтесь**, что...** проверены **окна использования для настройки**.
4. Если вы видите SSID в списке, нажмите **Configure**. В противном случае **нажмите Add**.
5. Вставьте SSID и проверьте **WEP**, и **Ключ предоставлен для меня автоматически**.
6. Выберите вкладку Authentication и удостоверьтесь**, включают контроль за сетевым доступом, использующий...** проверен.
7. Выберите **Protected EAP** и нажмите **Properties** для типа EAP.
8. Установите флажок для **CA** под Сертификатом доверенного корня.
9. **Нажмите OK** три раза.

Установите Windows XP для Сертификата (без SP1)

Выполните следующие действия:

1. Соединения Открытой сети на Панели управления и выбирают **Start> Control Panel**).
2. Щелкните правой кнопкой мыши беспроводную сеть и выберите **Properties**.
3. На вкладке Wireless Network удостоверьтесь**, что...** проверены **окна использования для настройки**.
4. Выберите вкладку Authentication и удостоверьтесь**, включают контроль за сетевым доступом, использующий...** проверен.
5. Выберите **PEAP** и нажмите **Properties** для типа EAP.
6. Установите флажок для **CA** под Сертификатом доверенного корня.
7. **Нажмите OK** три раза.

Установите Windows 2000 для PEAP

Выполните следующие действия:

1. Если вы выполняете SP3, загружаете и устанавливаете заплату 802.1x от Microsoft. Это не требуется для SP4.
2. Выберите **Start> Control Panel> Network и Dial-up Connections**.

3. Щелкните правой кнопкой мыши свое беспроводное соединение и выберите **Properties**.
4. Щелкните по вкладке Authentication.**Примечание:** Если нет никакой вкладки Authentication, сервис 802.1X установлен в отключенном состоянии. Для решения этого необходимо включить **сервис Конфигурации беспроводной сети** в списке сервисов:Щелкните правой кнопкой мыши **Мой компьютер** и нажмите **Manage**.**Choose Services> Приложения** и нажимает **Services**.Установите значение Запуска для сервиса к **Автоматическому**, и затем запустите сервис.**Примечание:** Если вкладка Authentication присутствует, но недоступна, это указывает, что драйвер сетевого адаптера не поддерживает 802.1x правильно. Проверьте список у основания страницы заплаты 802.1x или веб-узла поставщика для поддерживаемых драйверов.
5. Проверка **Включает управление доступом к сети с помощью IEEE 802.1x**.
6. Выберите **PEAP** из раскрывающегося меню типа EAP и нажмите **OK**.

При использовании ACU

Выполните следующие действия:

1. Откройте ACU.
2. Выберите **Manage Profile** и создайте профиль или отредактируйте тот.
3. Вставьте имя клиента и SSID AP.
4. Выберите Вкладку Сетевая безопасность.
5. Выберите **Host-based EAP for Network Security Type**.
6. Выберите **Use Dynamic WEP Keys for WEP**.
7. **Дважды нажмите кнопку OK.**
8. Выберите профиль, который вы создали.**Примечание:** При использовании соискателя Cisco на вкладке Authentication у вас только есть PEAP. При использовании Microsoft supplicant это сообщает EAP (PEAP).**Примечание:** Существует очень длинная задержка, прежде чем клиент попытается связаться к AP (приблизительно минута), который может быть частично облегчен с XP кумулятивного пакета беспроводного обновления для windows, доступное исправление от Microsoft. Это исправление может потенциально повторно установить EAP - соискатель MSCHAPv2, который препятствует тому, чтобы функционировали типы совместимой базы данных EAP-GTC.**Примечание:** Если вы не становитесь связанными, попытайтесь отключить и затем реактивировать карту.

Установите Windows 2003 Mobile для PEAP

Выполните следующие действия:

1. Установите последний выпуск Cisco ACU для Windows CE и обязательно установите инициатор запроса PEAP во время установки.
2. Откройте ACU и выберите **<Внешние Параметры настройки>** от Активного раскрывающегося меню Профиля.
3. Вставьте свою карту Сети Cisco, щелкните по значку сети на панели задач и выберите **Settings> Advanced> Network Card**.
4. Щелкните по своему SSID (при наличии) или **добавьте Новые Параметры настройки**.
5. Проверьте SSID в поле Network Name и сети для соединения с.
6. Щелкните по вкладке Authentication.

7. Проверьте **Шифрование данных (WEP)**, и **ключ предоставлен для меня....**”
8. Регистрация **Включает доступ к сети... 802.1x** и выбирает **Cisco PEAP**.
9. Нажмите **Properties**, и проверка **Проверяют** (дополнительный) **серверный сертификат**.**Примечание:** При проверке этой опции она требует, чтобы вы установили корневой сертификат CA на PocketPC. Windows Mobile не включает хороший метод, который можно использовать для импорта сертификатов. Существует много доступных утилит. Эти утилиты не поддерживаются Cisco. Импорт корневого сертификата CA вручную не требуется при использовании ACU так как инициатор запроса PEAP Cisco импортирует его для вас. Никакая версия подписанных сертификатов поддержек операционной системы PocketPC в это время, таким образом, вы не можете импортировать подписанные сертификаты в PocketPC для проверки. Можно все еще использовать подписанный сертификат при снятии выделения **с Проверить** опцией **серверного сертификата**.
10. Нажмите **OK**, пока вы не вернетесь в экране Configure Wireless Networks.
11. **Нажмите кнопку Connect (Подключить).**

Дополнение аутентификации компьютера

Цель аутентификации компьютера состоит в том, чтобы позволить Аутентификации eap и сетевому подключению быть установленной перед проверкой подлинности пользователя так, чтобы сценарии входа в систему могли работать, и пользователь может войти в систему домен. Членство в домене требуется для учетных данных машины быть установленным и аутентификация для имения место.

Установите ACS для Разрешения Аутентификации компьютера

Выполните следующие действия:

1. Выберите **External User Databases> Database Configuration**.
2. Нажмите **Windows Database** и выберите **Configure**.
3. Проверка **Включает аутентификацию компьютера PEAP**.
4. **Нажмите кнопку Submit (Отправить).**

Установите Client for Machine Authentification

Уже присоединитесь к Домену (если не участник домена)

Выполните следующие действия:

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 и нажмите **Change**.
4. Введите имя хоста в поле Computer Name (Имя компьютера).
5. Выберите **Domain**, введите имя домена и нажмите **OK**.
6. Для присоединения к домену диалоговое окно входа в систему отображается. Вход в систему с учетной записью, которая имеет разрешения для присоединения к домену.
7. Как только компьютер успешно присоединяется к домену, перезапустите компьютер.

Машина является участником домена и выполнила согласование об учетных данных для аутентификации с доменом, которые только известны ОС. В Cisco Secure ACS имя пользователя появляется как хост/имя хоста.

Установите Инициатор запроса PEAP для Аутентификации компьютера

Выполните следующие действия:

1. Выберите **Start> Control Panel** чтобы к Соединениям открытой сети на панели управления.
2. Щелкните правой кнопкой мыши сетевое подключение и выберите **Properties**.
3. Выберите вкладку Authentication, и проверка **Аутентифицируются как компьютер**.

Дополнение управления ключами WPA

Записанный для Cisco IOS AP 12.02 (13) JA1, Cisco Secure ACS 3.2, и Windows XP SP1 с исправлением WPA.

Примечание: Клиенты Windows 2000 исходно не поддерживают управление ключами WPA. Необходимо использовать клиентское программное обеспечение поставщика для получения этой поддержки:

Примечание: Cisco ACU не поддерживает управление ключами WPA для основанного на хосте EAP (EAP-TLS и PEAP) в это время. Необходимо установить клиента третьей стороны, такого как фанковый Клиент Odyssey или Клиент aegis Meetinghouse. См. Поддержку WPA для получения дополнительной информации о WPA поддерживают для продуктов Cisco.

Примечание: Также обратите внимание, что драйверы, установленные для карт Cisco карманной ПК версией ACU, не поддерживают WPA в это время. WPA не работает для клиентов Cisco на PocketPC даже с соискателем Третьей стороны.

Настройте AP

Выполните следующие действия:

1. **Выберите Security > Encryption Manager.Шифр ChooseWEP** и выбирает **TKIP** из выпадающего.**Щелкните "Применить".**
2. **Выберите Security > SSID Manager.**Выберите SSID из Текущего Списка SSID или введите новый SSID в поле SSID.Проверьте **Открытую аутентификацию** и выберите **с EAP** из раскрывающегося меню.Проверьте **сетевой EAP**.Под Аутентифицируемым Управлением ключами выберите **Mandatory** из раскрывающегося меню и нажмите **WPA**.**Щелкните "Применить".**

Установите Windows XP SP1 (с установленным KB826942) или Клиент SP2 для PEAP и WPA

Выполните следующие действия:

1. Выберите **Start> Control Panel** чтобы к Соединениям открытой сети на панели управления.
2. Щелкните правой кнопкой мыши беспроводную сеть и выберите **Properties**.
3. На вкладке Wireless Network удостоверьтесь**, что...** проверены **окна использования для настройки**.
4. Если вы видите SSID в списке, нажмите **Configure**. В противном случае **нажмите Add**.
5. Вставьте SSID и выберите **WPA for Network Authentication** и **TKIP for Data Encryption**.
6. Выберите вкладку Authentication и удостоверьтесь, что **включают контроль за сетевым доступом, использующий...** проверен.
7. Выберите **Protected EAP** и нажмите **Properties** для типа EAP.
8. Установите флажок для **CA** под Сертификатом доверенного корня.
9. **Нажмите OK** три раза.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Проблема 1

Эта ошибка происходит во время установки сертификатов / аутентификация с ACS.

```
Unsupported private key file format
Failed to initialize PEAP or EAP-TLS authentication protocol because ACS certificate is
not installed
```

Решение

Ошибка происходит, потому что peap сертификат не установлен properally. Удалите сертификат и установите новый подписанный сертификат для решения проблемы.

Проблема 2

Эта ошибка происходит во время установки сертификатов / аутентификация с ACS.

```
Failed to initialize PEAP or EAP-TLS authentication protocol because CA certificate is
 not installed.
```

Решение

Для решения ошибки установите сертификат CA с помощью Настройки Центра сертификации ACS. Если подписанный сертификат не используется, эта ошибка происходит из-за неправильного сертификата CA.

Проблема 3

Когда обновление ACS сделано, эта ошибка происходит.

```
A required certificate is not within its validity period when verifying
```

```
against the current system clock or the timestamp in the signed file.
(800B0101)
```

Решение

Эта ошибка происходит, когда обновление программного обеспечения ACS сделано, если вы не обновляете Программное обеспечение для управления. Выполните обновление Программного обеспечения для управления и затем обновление программного обеспечения ACS для решения проблемы. См. Обновление раздела Устройства Администрирования Устройства Cisco Secure ACS для получения дополнительной информации о том, как обновить ACS.

Проблема 4

Эта ошибка происходит во время установки сертификатов с ACS.

```
Private key you've selected doesn't fit to this certificate
```

Решение

Наиболее распространенная причина этого случайно перезаписывает секретный ключ, генерируют новый CSR.

Проверьте эту информацию:

1. Вы загружаете корректный сертификат как сертификат ACS.
2. Длина ключа паба RSA составляет 1024 бита во время создания запроса.
3. Вы используете завершенный CN=string при генерации CSR.

Дополнительные сведения

- Страница поддержки Cisco Secure ACS для UNIX
- Уведомления о дефектах продуктов безопасности (включая CiscoSecure UNIX)
- Документация для сервера управления безопасного доступа Cisco для Unix
- Страница поддержки Cisco Secure ACS для Windows
- Документация по Cisco Secure ACS для Windows
- Cisco Systems – техническая поддержка и документация