

Настройка Cisco Secure ACS для Windows v3.2 с проверкой подлинности компьютеров PEAP-MS-CHAPv2

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Теоретические сведения](#)

[Условные обозначения](#)

[Схема сети](#)

[Настройте Cisco Secure ACS для Windows v3.2](#)

[Получение сертификата для сервера ACS](#)

[Настройте ACS для использования сертификата из хранилища](#)

[Указание дополнительных СА, которым должен доверять сервер ACS](#)

[Перезапустите эту службу и настройте параметры PEAP на ACS](#)

[Указание и настройка точки доступа в качестве клиента AAA](#)

[Настройте внешние базы данных пользователей](#)

[Перезапустите службу](#)

[Настройте точку доступа Cisco](#)

[Настройте беспроводного клиента](#)

[Настройте автоматическую регистрацию сертификатов MS](#)

[Подключитесь к домену](#)

[Вручную установить сертификат корня на клиенте Windows](#)

[Настройте беспроводной доступ к сети](#)

[Проверка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

Введение

В этом документе демонстрируется настройка протокола аутентификации PEAP с Cisco Secure ACS для Windows 3.2.

Для получения дополнительной информации о том, как настроить безопасный беспроводной доступ с помощью Контроллеров беспроводной локальной сети, программного обеспечения Microsoft Windows 2003 и сервера Cisco Secure Access Control Server (ACS) 4.0, обратитесь к [PEAP под Unified Wireless Network с ACS 4.0 и Windows 2003](#).

Предварительные условия

Требования

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Сведения в этом документе основаны на версиях оборудования и программного обеспечения, указанных ниже.

- Cisco Secure ACS для Windows (версия 3.2)
- Сервисы сертификации Microsoft (установленные как корневой CA предприятия)**Примечание:** [Дополнительные сведения см. в пошаговом руководстве по установке центра сертификации \(CA\).](#)
- Служба DNS в Windows 2000 Server с установленным пакетом обновлений Service Pack 3**Примечание:** [Если есть проблемы с сервером CA, установите hotfix 323172. Клиенту Windows 2000 SP3 необходим hotfix 313664 для активации аутентификации IEEE 802.1x.](#)
- Беспроводная точка доступа Cisco Aironet серии 1200 (версия 12.01T)
- IBM ThinkPad T30 под управлением Windows XP Professional с пакетом обновления 1

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Теоретические сведения

Как PEAP, так и EAP-TLS устанавливают и используют туннель TLS/Secure Socket Layer (SSL). PEAP использует только серверную аутентификацию, только у сервера есть сертификат и только сервер доказывает свою подлинность клиенту. EAP-TLS использует взаимную аутентификацию, при которой и сервер управления доступом (аутентификация, авторизация и учет [AAA]) и клиенты имеют сертификаты и удостоверяют личности друг друга.

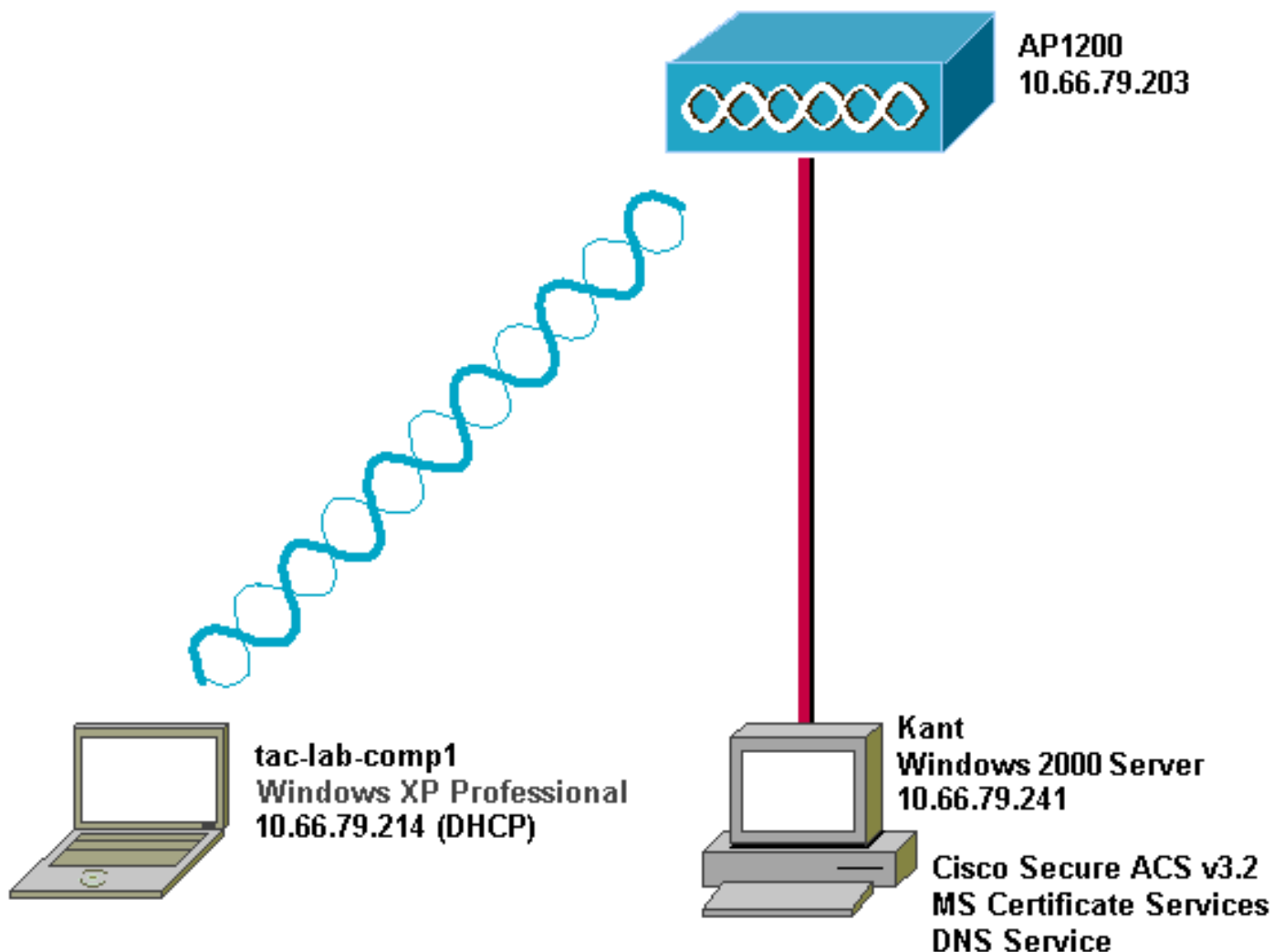
PEAP удобен в использовании, так как клиентам не нужны сертификаты. EAP-TLS полезен для автономных устройств, осуществляющих аутентификацию, так как сертификаты не требуют вмешательства пользователя.

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.](#)

Схема сети

В данном документе используется сетевая установка, показанная на следующей схеме.



Настройте Cisco Secure ACS для Windows v3.2

Выполните эти действия для настройки ACS 3.2.

1. [Получение сертификата для сервера ACS.](#)
2. [Настройте ACS для использования сертификата из хранилища.](#)
3. [Указание дополнительных CA, которым должен доверять сервер ACS.](#)
4. [Перезапустите эту службу и настройте параметры PEAP на ACS.](#)
5. [Указание и настройка точки доступа в качестве клиента AAA.](#)
6. [Настройте внешние базы данных пользователей.](#)
7. [Перезапустите службу.](#)

Получение сертификата для сервера ACS

Чтобы получить сертификат, выполните данные шаги.

1. *На сервере системы усовершенствованных коммуникаций откройте браузер и просмотрите сервер сертификации, перейдя по адресу <http://CA-ip-address/certsrv>. Войдите в домен с правами администратора.*

Enter Network Password [?] [X]

 Please type your user name and password.

Site: 10.66.79.241

User Name: Administrator

Password: *****

Domain: SEC-SYD

Save this password in your password list

OK Cancel

2. Выберите пункт **Request a certificate (Запрос сертификата)**, затем нажмите кнопку **Next**

Microsoft Certificate Services -- Our TAC CA [Home](#)

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

Next >

(Далее).

3. Выберите **Advanced request (Расширенный запрос)** и нажмите кнопку **Next**

Choose Request Type

Please select the type of request you would like to make:

User certificate request:

Advanced request

Next >

(Далее).

4. Выберите Submit a certificate request to this CA using a form (Отправить запрос сертификата этому центру посредством формы) и нажмите кнопку Next

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

- Submit a certificate request to this CA using a form.
- Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.
- Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

Next >

(Далее).

5. Настройте параметры сертификата. **Выберите веб-сервер в качестве шаблона сертификата.** Введите имя ACS-

Advanced Certificate Request

Certificate Template:

Identifying Information For Offline Template:

сервера.

Укажите для размера ключа значение 1024. Выберите параметры для "Пометить ключи как разрешенные для экспорта" и "Использовать хранилище локального компьютера". Настройте остальные параметры необходимым образом и нажмите кнопку Подтвердить.

Key Options:

CSP:

Key Usage: Exchange Signature Both

Key Size: Min: 384 Max: 1024 (common key sizes: [512](#) [1024](#))

Create new key set
 Set the container name

Use existing key set

Enable strong private key protection

Mark keys as exportable
 Export keys to file

Use local machine store
You must be an administrator to generate a key in the local machine store.

Additional Options:

Hash Algorithm: Only used to sign request.

Save request to a PKCS #10 file

Attributes:

Примечание:

Если появится окно предупреждения о нарушении сценария (в зависимости от настроек безопасности/секретности браузера), щелкните Yes (Да), чтобы




продолжить.

- Нажмите кнопку Install this certificate (Установить этот сертификат).

Microsoft Certificate Services -- Our TAC CA [Home](#)

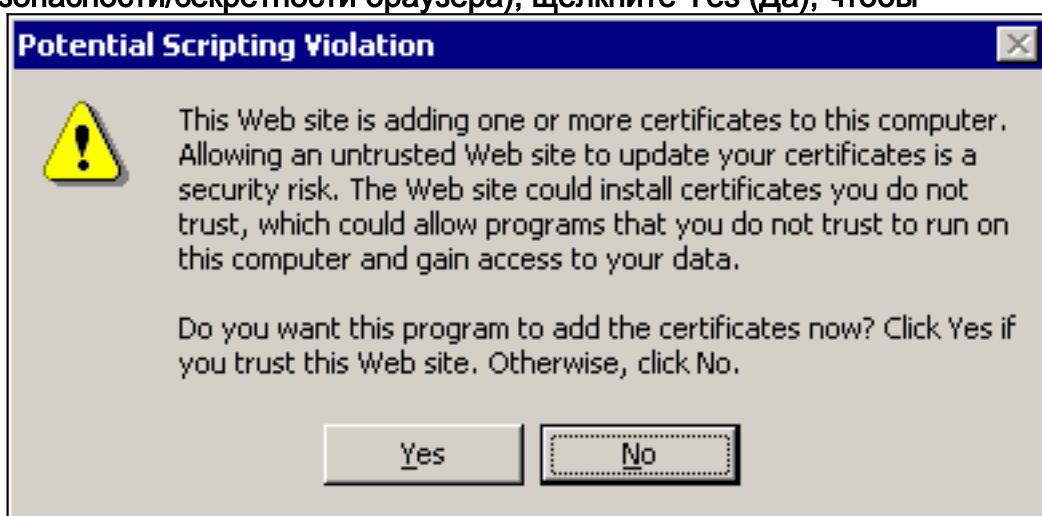
Certificate Issued

The certificate you requested was issued to you.

 [Install this certificate](#)

Примечание:

Если появится окно предупреждения о нарушении сценария (в зависимости от настроек безопасности/секретности браузера), щелкните Yes (Да), чтобы



продолжить.

7. В случае успешной инсталляции появляется подтверждающее сообщение.

Microsoft Certificate Services -- Our TAC CA [Home](#)

Certificate Installed

Your new certificate has been successfully installed.

[Настройте ACS для использования сертификата из хранилища](#)

Выполните следующие действия, чтобы настроить ACS для использования сертификата из хранилища.

1. Откройте браузер сети и введите в строку адреса `http://ACS-ip-address:2002/`. В разделе System Configuration (Настройка системы) выберите ACS Certificate Setup (Настройка сертификатов управления доступом).
2. Нажмите кнопку Install ACS certificate (Установить сертификат ACS).

3. Выберите вариант использования сертификата из хранилища. В поле Certificate CN введите имя сертификата, который вы назначили в шаге 5а раздела, [Получают Сертификат для Сервера ACS](#). Нажмите кнопку Submit (Отправить). Эта запись должна совпадать с именем, введенным в поле "Name" во время расширенного запроса сертификата. В предметном поле сертификата сервера находится имя CN, сертификат сервера можно редактировать, установив флажок возле этого имени. В данном примере сервер контроля доступа называется "OurACS". Не вводить имя CN выдающей

The screenshot shows the Cisco System Configuration web interface. The left sidebar contains navigation menus: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration (highlighted), Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "System Configuration" and "Edit". The current page is "Install ACS Certificate". Under the heading "Install new certificate", there are two radio button options: "Read certificate from file" and "Use certificate from storage". The "Use certificate from storage" option is selected and circled in red. Below this, the "Certificate CN" field is filled with "OurACS" and is also circled in red. Other fields include "Certificate file", "Private key file", and "Private key password", all of which are currently empty. A "Back to Help" button is located below the form. At the bottom of the page, there are "Submit" and "Cancel" buttons.

службы.

4. После завершения настройки будет выведено сообщение о подтверждении, указывающее, что конфигурация сервера ACS была изменена. **Примечание:** Перезапуск сервера управления доступом не

CISCO SYSTEMS

System Configuration

Edit

Install ACS Certificate

Installed Certificate Information ?

Issued to: OurACS
Issued by: Our TAC CA
Valid from: June 23 2003 at 02:19:56
Valid to: June 18 2005 at 00:52:30
Validity: OK

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

Install New Certificate Cancel

требуется.

[Указание дополнительных СА, которым должен доверять сервер ACS](#)

Сервер управления доступом (ACS) автоматически доверяет центрам сертификации, которые выпускают собственный сертификат. Если сертификат клиента выпущен дополнительными центрами сертификации, то необходимо выполнить следующие шаги.

1. В разделе System Configuration (Настройка системы) выберите ACS Certificate Setup (Настройка сертификатов управления доступом).
2. Щелкните ACS Certificate Authority Setup (Установка центра сертификации ACS), чтобы добавить центр сертификации к списку доверенных сертификатов. В соответствующее поле введите расположение файла сертификата СА и нажмите кнопку Submit (Отправить).

The screenshot shows the Cisco System Configuration interface. At the top left is the Cisco Systems logo. The main title is "System Configuration". Below the title is a black bar with the word "Edit" in white. On the left side, there is a vertical navigation menu with icons and labels for various configuration areas: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "ACS Certification Authority Setup". Below this title is a section titled "CA Operations" with a help icon. The text below reads "Add new CA certificate to local certificate storage". There is a text input field labeled "CA certificate file". Below the input field is a yellow button with a help icon and the text "Back to Help".

- Щелкните **Edit Certificate Trust List** (Редактировать список доверенных сертификатов). Установите флажки для всех центров сертификации, которым должен доверять сервер управления доступом, и снимите флажки для всех центров, которым он не должен доверять. Нажмите кнопку **Submit** (Отправить).

CISCO SYSTEMS

System Configuration

Edit

Edit Certificate Trust List

Edit the Certificate Trust List (CTL)

Display Name (Friendly Name)

- ABA.ECOM Root CA
(DST (ABA.ECOM) CA)
- Autoridad Certificadora de la Asociacion Na
(Autoridad Certificadora de la Asociacion N)
- Autoridad Certificadora del Colegio Naciona
- Baltimore EZ by DST
(DST (Baltimore EZ) CA)
- Belgacom E-Trust Primary CA
- C&W HKT SecureNet CA Class A
(CW HKT SecureNet CA Class A)
- C&W HKT SecureNet CA Class B
(CW HKT SecureNet CA Class B)

[Перезапустите эту службу и настройте параметры PEAP на ACS](#)

Выполните эти действия, чтобы перезапустить сервис и настроить параметры настройки PEAP.

1. В разделе System Configuration (Настройка системы) выберите Service Control (Управление службами).
2. Нажать Restart для того, чтобы перезапустить службу.
3. Для настройки параметров PEAP выберите компонент "Настройка системы", а затем "Настройка глобальной аутентификации".
4. Проверьте две настройке, показанные ниже, и оставьте значения всех остальных настроек по умолчанию. Можно задать дополнительные параметры, например Enable Fast Reconnect. По завершении нажмите кнопку "Отправить".**Разрешить EAP-MSCHAPv2Allow MS-CHAP Version 2 Authentication**Примечание: [Дополнительную информацию по функции быстрого установления соединения Fast Connect см. в подразделе "Параметры конфигурации аутентификации" раздела "Конфигурация системы": Проверка подлинности и сертификаты.](#)

