

# Безопасный ACS для Windows v3.2 With EAP-TLS Machine Authentication

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Теоретические сведения](#)

[Условные обозначения](#)

[Схема сети](#)

[Настройка Cisco Secure ACS версии 3.2 для Windows](#)

[Получение сертификата для сервера ACS](#)

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

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

[Перезапуск службы и настройка параметров EAP-TLS на сервере ACS](#)

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

[Настройте внешние базы данных пользователей](#)

[Перезапустите службу](#)

[Настройка автоматического зачисления сертификата Microsoft для компьютера](#)

[Настройка точки доступа Cisco](#)

[Настройка беспроводного клиента](#)

[Подключитесь к домену](#)

[Получение сертификата для пользователя](#)

[Настройте беспроводной доступ к сети](#)

[Проверка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

## Введение

Этот документ описывает, как настроить Transport Layer Security расширяемого протокола аутентификации (EAP-TLS) с системой управления доступом Cisco Secure Access Control System (ACS) для Версии Windows 3.2.

**Примечание:** Аутентификация компьютера не поддерживается с Центром сертификации (CA) Novell. Сервер ACS может использовать EAP-TLS для поддержки аутентификации компьютеров в каталоге Active Directory системы Microsoft Windows. Клиент конечного пользователя может ограничивать выбор протоколов аутентификации пользователя только тем протоколом, который используется для аутентификации компьютеров. Таким образом, использование EAP-TLS для аутентификации компьютеров может потребовать применения

EAP-TLS для аутентификации пользователей. [Дополнительные сведения об аутентификации компьютеров см. в разделе Аутентификация компьютеров Руководства пользователя сервера управления доступом Cisco 4.1.](#)

**Примечание:** Когда устанавливается ACS для аутентификации машин через EAP-TLS и ACS было установлено для Аутентификации компьютера, клиент должен быть настроен, чтобы сделать аутентификацию компьютера только. Для получения дополнительной информации обратитесь [Как включить аутентификацию только для компьютера для основанной на 802.1X сети в Windows Vista в Windows Server 2008, и в Windows XP Service Pack 3.](#)

## 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 с Windows 2000 Server с пакетом обновления SP3 и исправлением 323172](#)**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

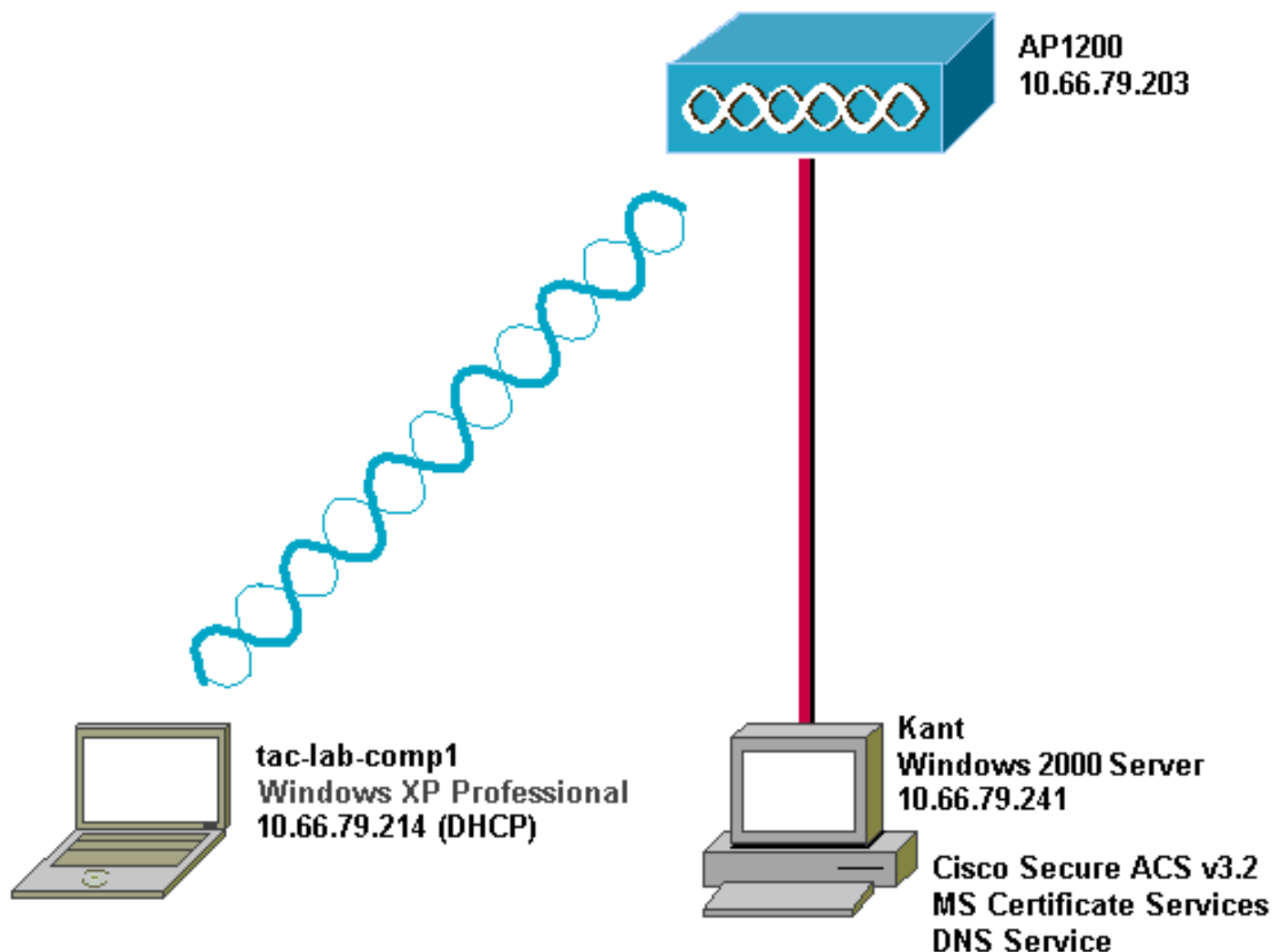
И EAP-TLS, и защищенный расширяемый протокол аутентификации (PEAP) образуют и используют туннель TLS/Secure Socket Layer (SSL). EAP-TLS использует взаимную аутентификацию, при которой сервер управления доступом (AAA) и клиенты имеют сертификаты и удостоверяют личности друг друга. В то же время, PEAP использует только серверную аутентификацию, только у сервера есть сертификат и только сервер доказывает свою подлинность клиенту.

### 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.



## Настройка Cisco Secure ACS версии 3.2 для Windows

Для настройки ACS 3.2 следуйте указанным ниже инструкциям.


1. [Получение сертификата для сервера ACS.](#)
2. [Настройте ACS для использования сертификата из хранилища.](#)
3. [Указание дополнительных СА, 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 ACS откройте браузер и войдите на сервер центра сертификации, набрав адрес <http://ip-адрес-центра-сертификации/certsrv>.*

2. Войдите в домен с правами администратора.



**Enter Network Password**

Please type your user name and password.

Site: 10.66.79.241

User Name: Administrator

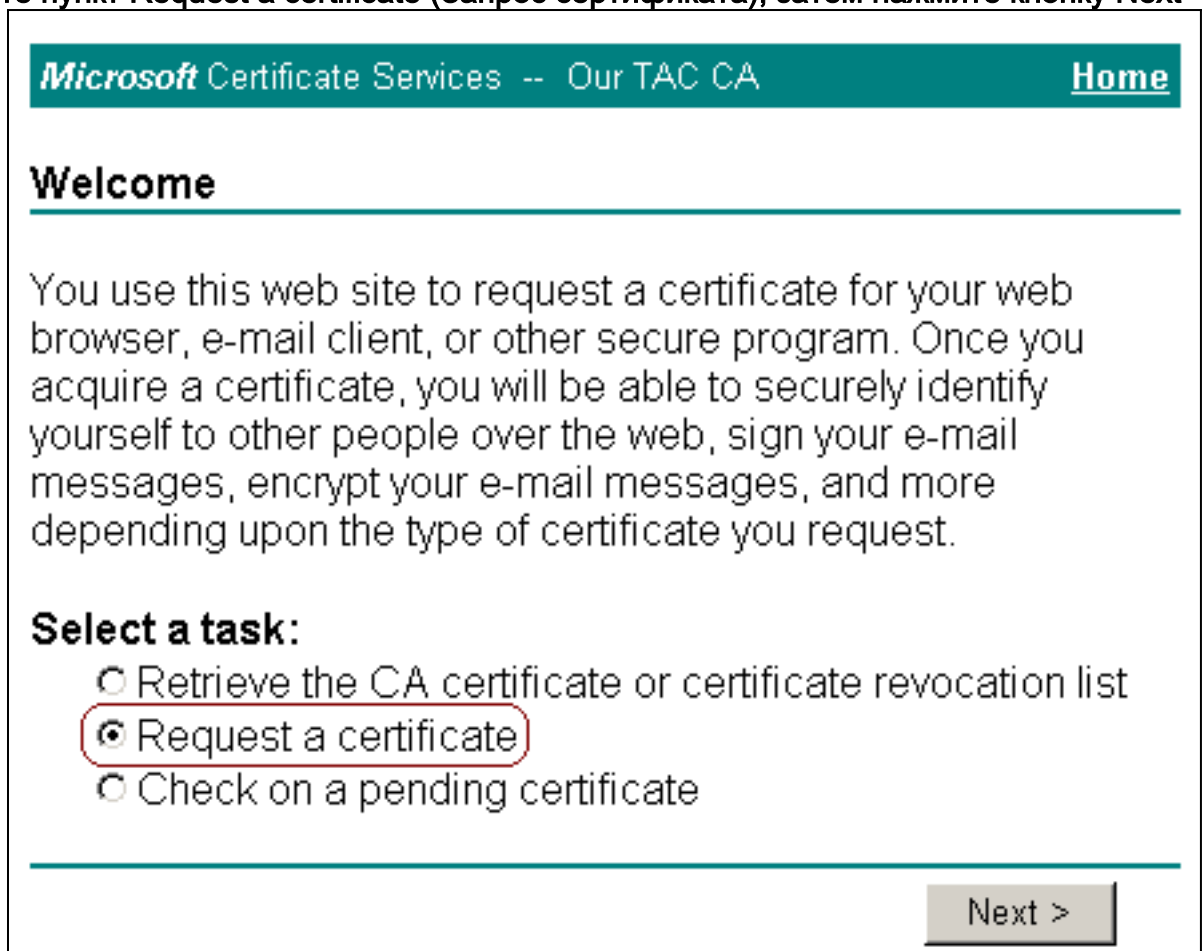
Password: \*\*\*\*\*

Domain: SEC-SYD

Save this password in your password list

OK Cancel

3. 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).

4. 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).

5. 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).

6. Настройте параметры сертификата: **В качестве шаблона сертификата выберите Web Server (web-сервер) и введите имя сервера**

## Advanced Certificate Request

### Certificate Template:

### Identifying Information For Offline Template:

ACS.

B

поле Key Size (Размер ключа) введите 1024, затем отметьте флажки Mark keys as exportable (Пометить ключи как экспортируемые) и Use local machine store (Использовать локальное хранилище компьютера). Настройте остальные параметры необходимым образом и нажмите кнопку Подтвердить.

### Key Options:

CSP: Microsoft Base Cryptographic Provider v1.0

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:

Submit >

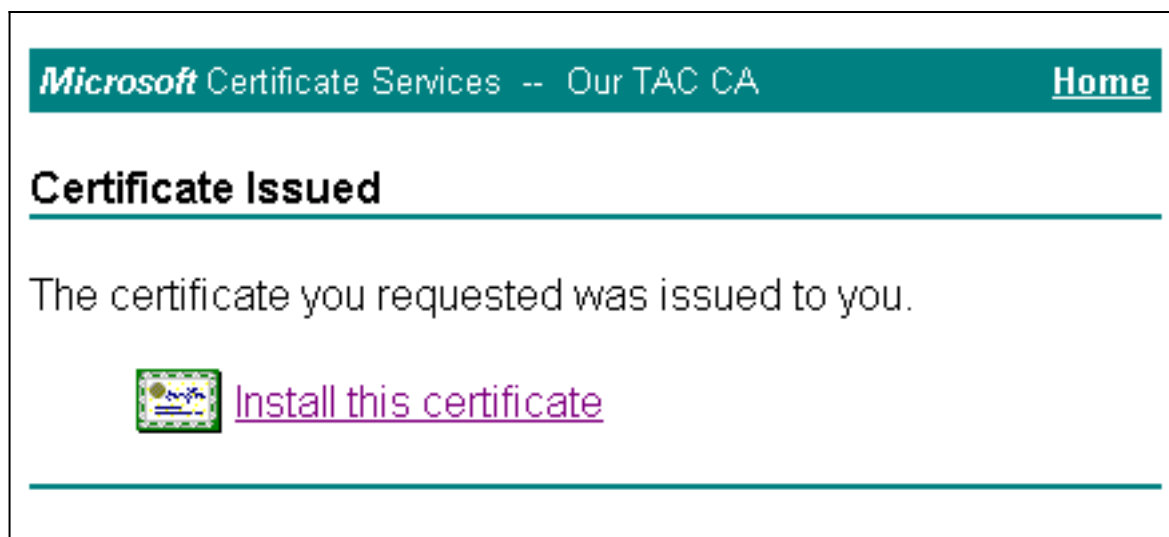
Примечание: Если диалоговое окно Potential Scripting Violation появляется, нажмите **Yes** для



продолжения.

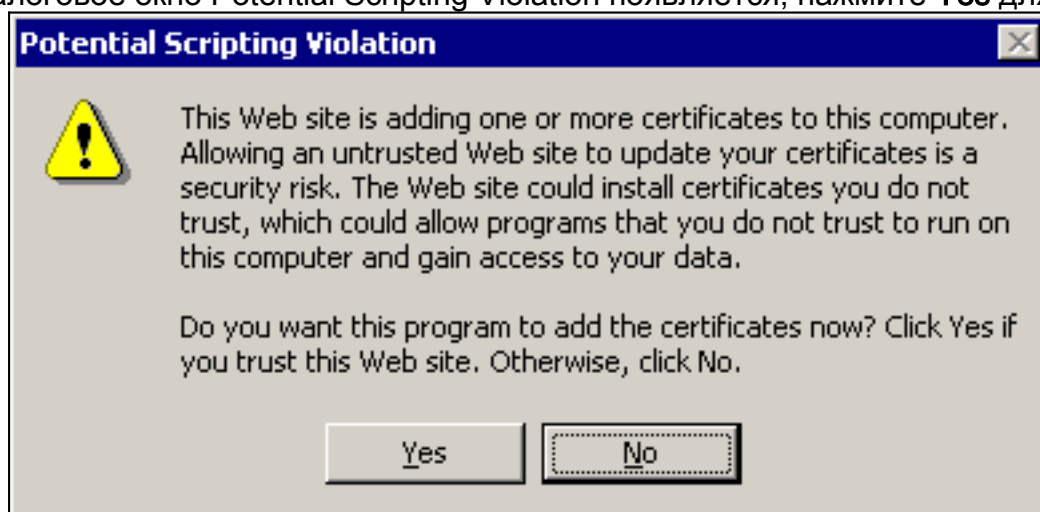
7. Нажмите кнопку **Install this certificate** (Установить этот сертификат).





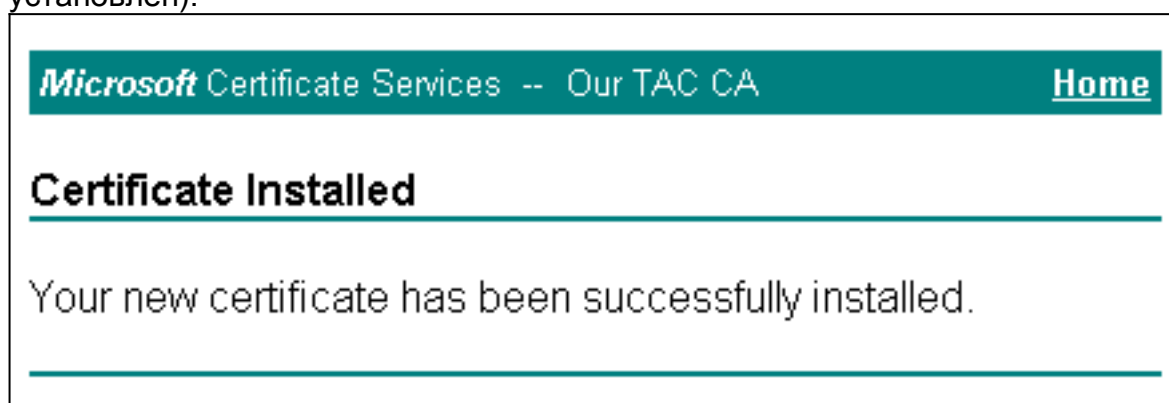
Примечание:

Если диалоговое окно Potential Scripting Violation появляется, нажмите **Yes** для



продолжения.

8. В случае успешной установки появится сообщение Certificate Installed (Сертификат установлен).



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

Чтобы настроить ACS для использования сертификата из хранилища, выполните следующие действия.

1. Для доступа к серверу ACS откройте браузер и введите: *http://ip-адрес-ACS:2002/*.
2. В разделе System Configuration (Настройка системы) выберите ACS Certificate Setup (Настройка сертификатов управления доступом).
3. Нажмите кнопку Install ACS certificate (Установить сертификат ACS).
4. Нажмите кнопку Use certificate from storage (Использовать сертификат из хранилища).

5. В поле Certificate CN (Общее имя сертификата) введите имя сертификата, назначенного в пункте 5а раздела Получение сертификата от сервера ACS настоящего документа.
6. Нажмите кнопку Submit (Отправить).

The screenshot shows the Cisco Systems System Configuration 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'. Below this is the 'Install ACS Certificate' section. A sub-section titled 'Install new certificate' contains two radio button options: 'Read certificate from file' and 'Use certificate from storage' (which is selected and circled in red). Below the selected option is a text field for 'Certificate CN' containing the value 'OurACS'. Further down are text fields for 'Private key file' and 'Private key password'. At the bottom of the form area is a yellow 'Back to Help' button. At the very bottom of the page are 'Submit' and 'Cancel' buttons.

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.

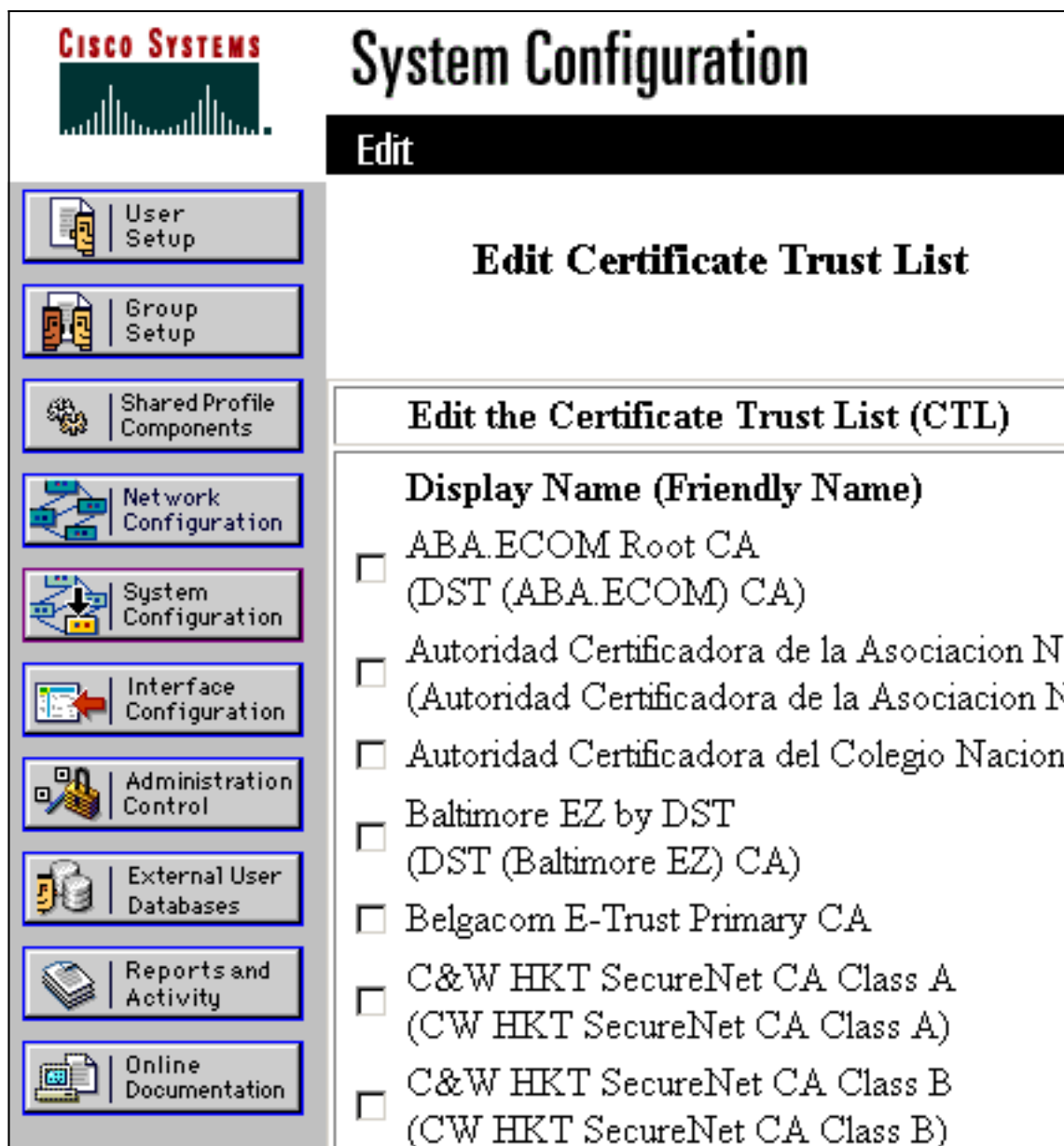
### [Указание дополнительных СА, которым должен доверять сервер ACS](#)

Сервер управления доступом (ACS) автоматически доверяет центру сертификации, выпустившему его сертификат. Если сертификаты клиента выпущены иным центром 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.
3. 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 the following items: "User Setup", "Group Setup", "Shared Profile Components", "Network Configuration", "System Configuration" (highlighted in purple), "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 question mark icon and the text "Back to Help".

4. Щелкните **Edit Certificate Trust List** (Редактировать список доверенных сертификатов).
5. Установите флажки для всех центров сертификации, которым должен доверять сервер управления доступом, и снимите флажки для всех центров, которым он не должен доверять.
6. 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)

## [Перезапуск службы и настройка параметров EAP-TLS на сервере ACS](#)

Для перезапуска службы и настройки параметров EAP-TLS следуйте приведенным ниже указаниям:

1. В разделе System Configuration (Настройка системы) выберите Service Control (Управление службами).
2. Нажмите кнопку Restart (Перезапуск), чтобы перезапустить службу.
3. Для настройки параметров PEAP выберите System Configuration (Настройка системы), а затем –Global Authentication Setup (Глобальная настройка аутентификации).
4. Отметьте флажок Allow EAP-TLS (Разрешить EAP-TLS), а затем один или несколько сравниваемых сертификатов.
5. Нажмите кнопку Submit (Отправить).

