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

## Содержание



## 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.

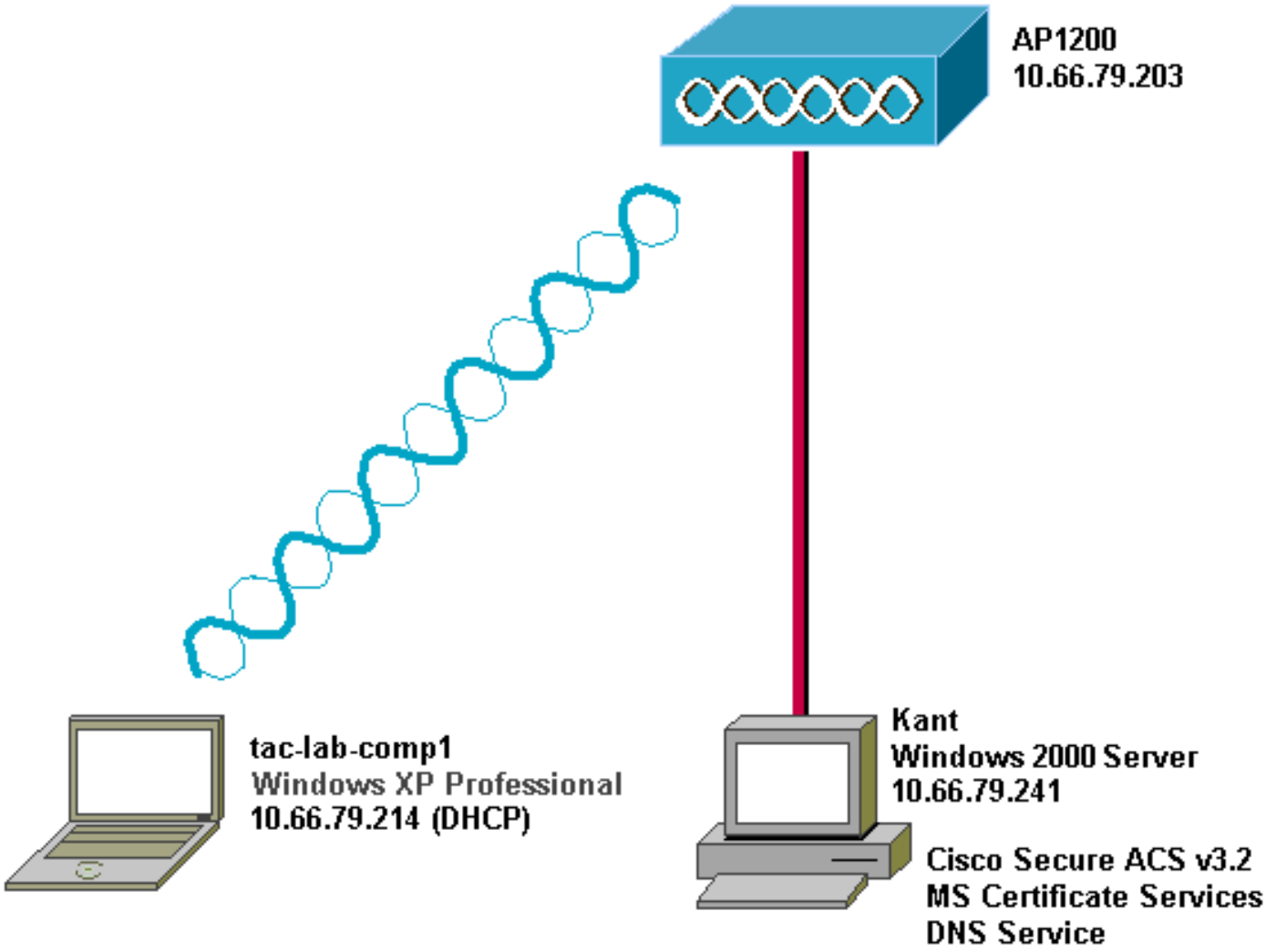
PEAP удобен в использовании, так как клиентам не нужны сертификаты. EAP-TLS полезен для автономных устройств, осуществляющих аутентификацию, так как сертификаты не требуют вмешательства пользователя.

## 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

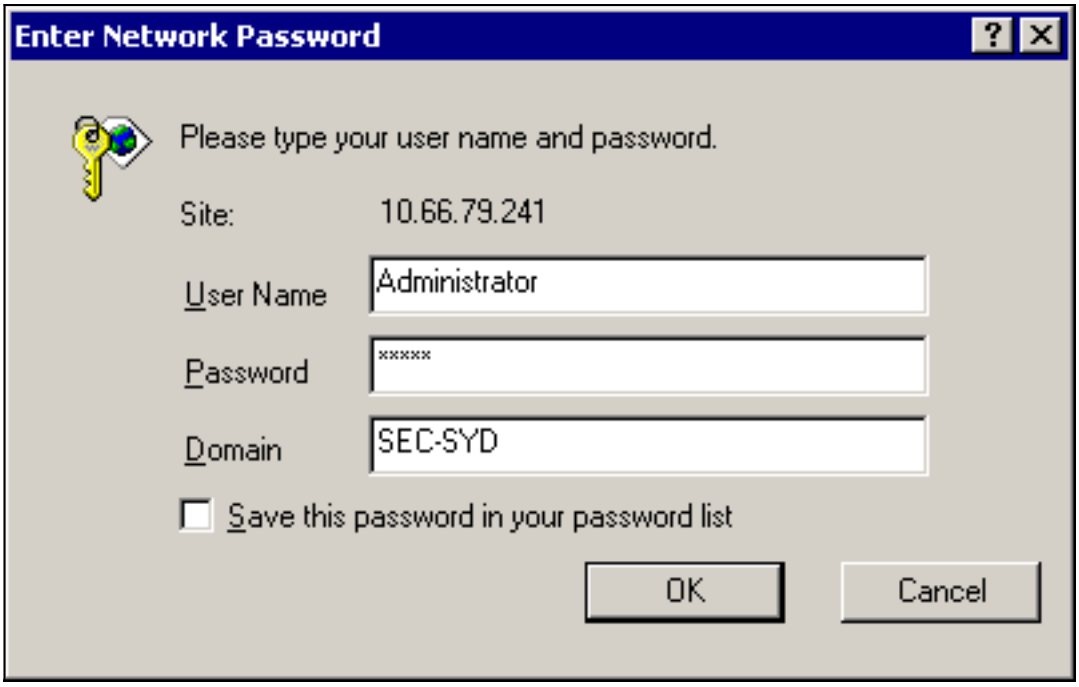
Выполните эти действия для настройки ACS 3.2.

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.

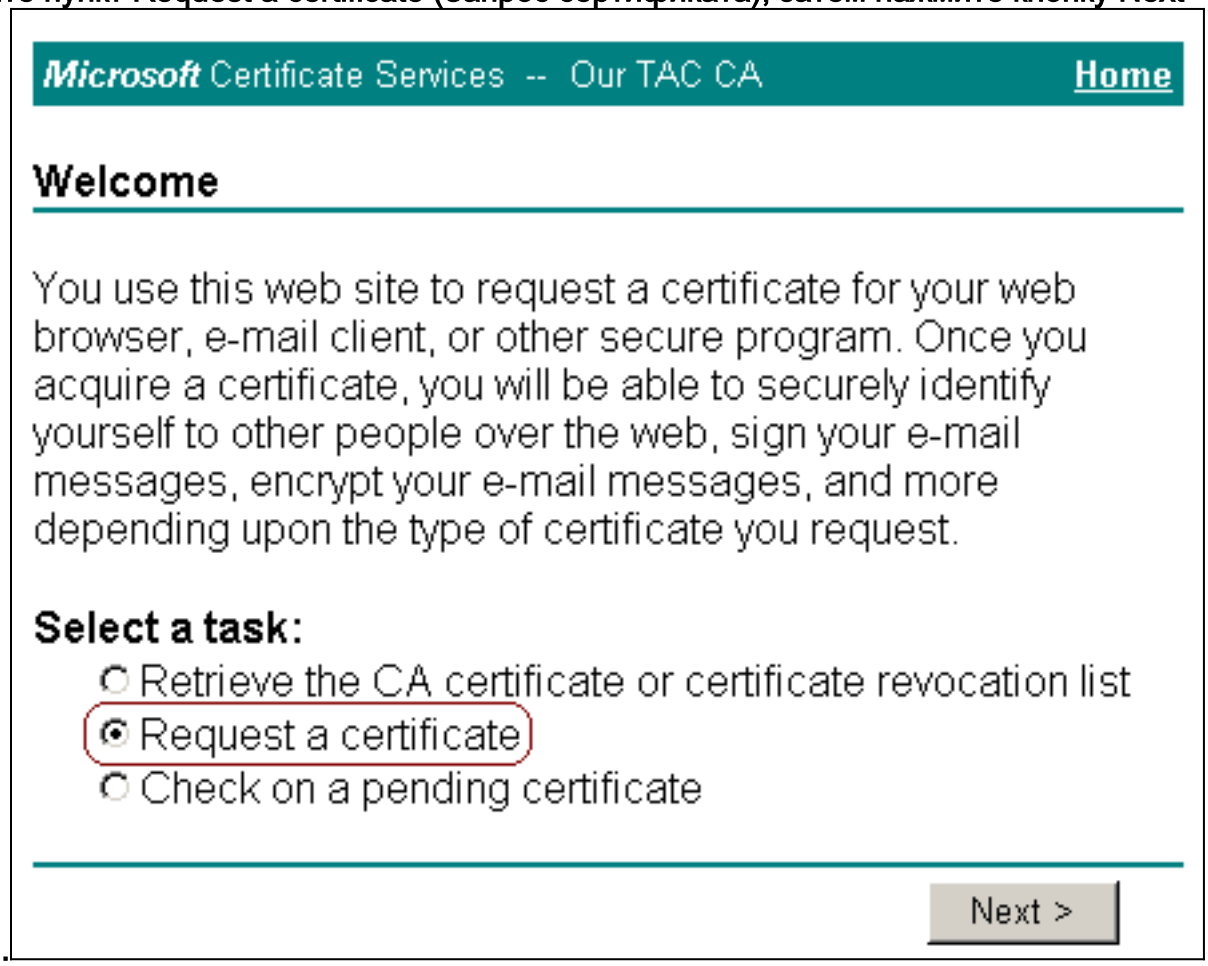
## Получение сертификата для сервера ACS

Чтобы получить сертификат, выполните данные шаги.

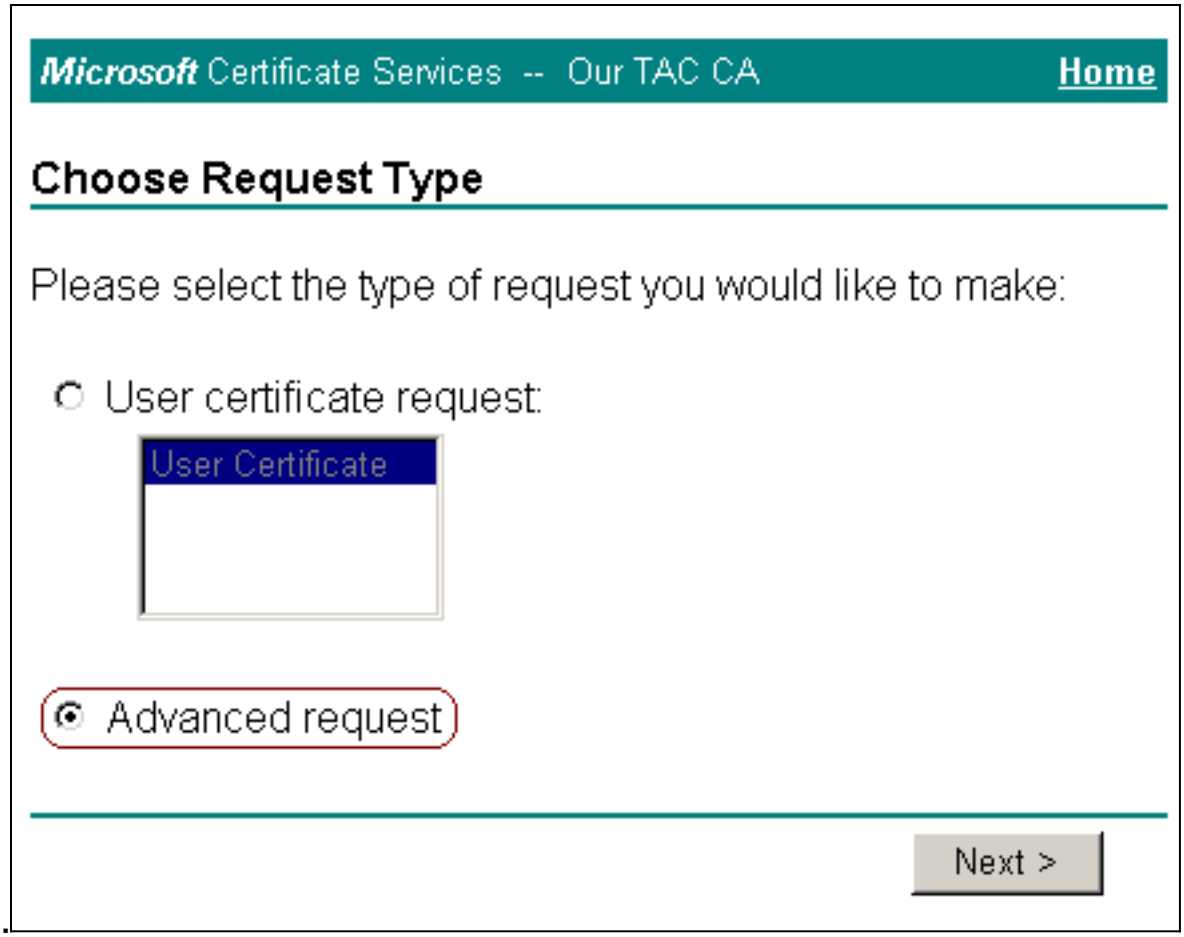
1. *На сервере системы усовершенствованных коммуникаций отройте браузер и просмотрите сервер сертификации, перейдя по адресу http://CA-ip-address/certsrv.* Войдите в домен с правами администратора.




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

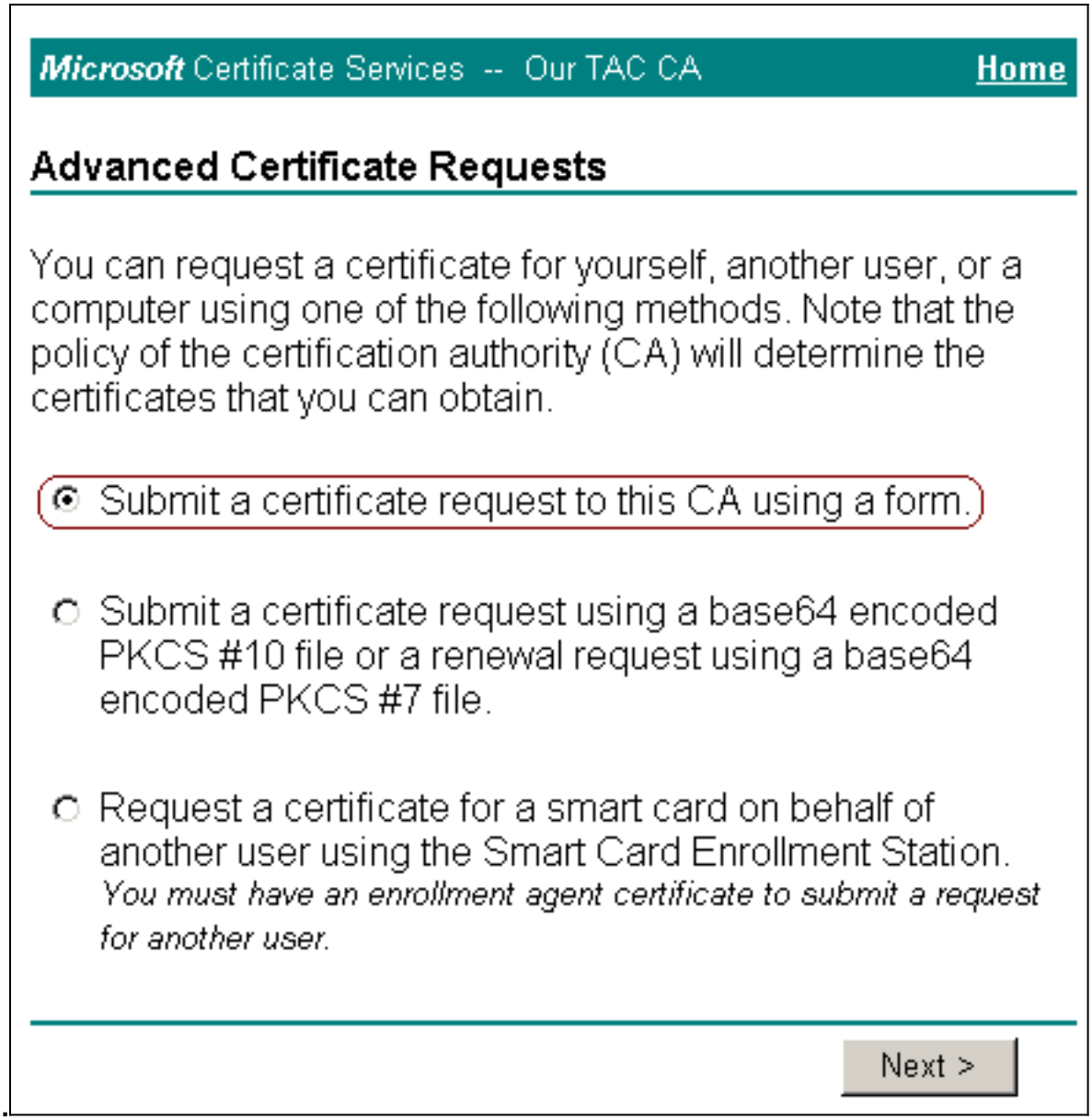



3. Выберите Advanced request (Расширенный запрос) и нажмите кнопку Next



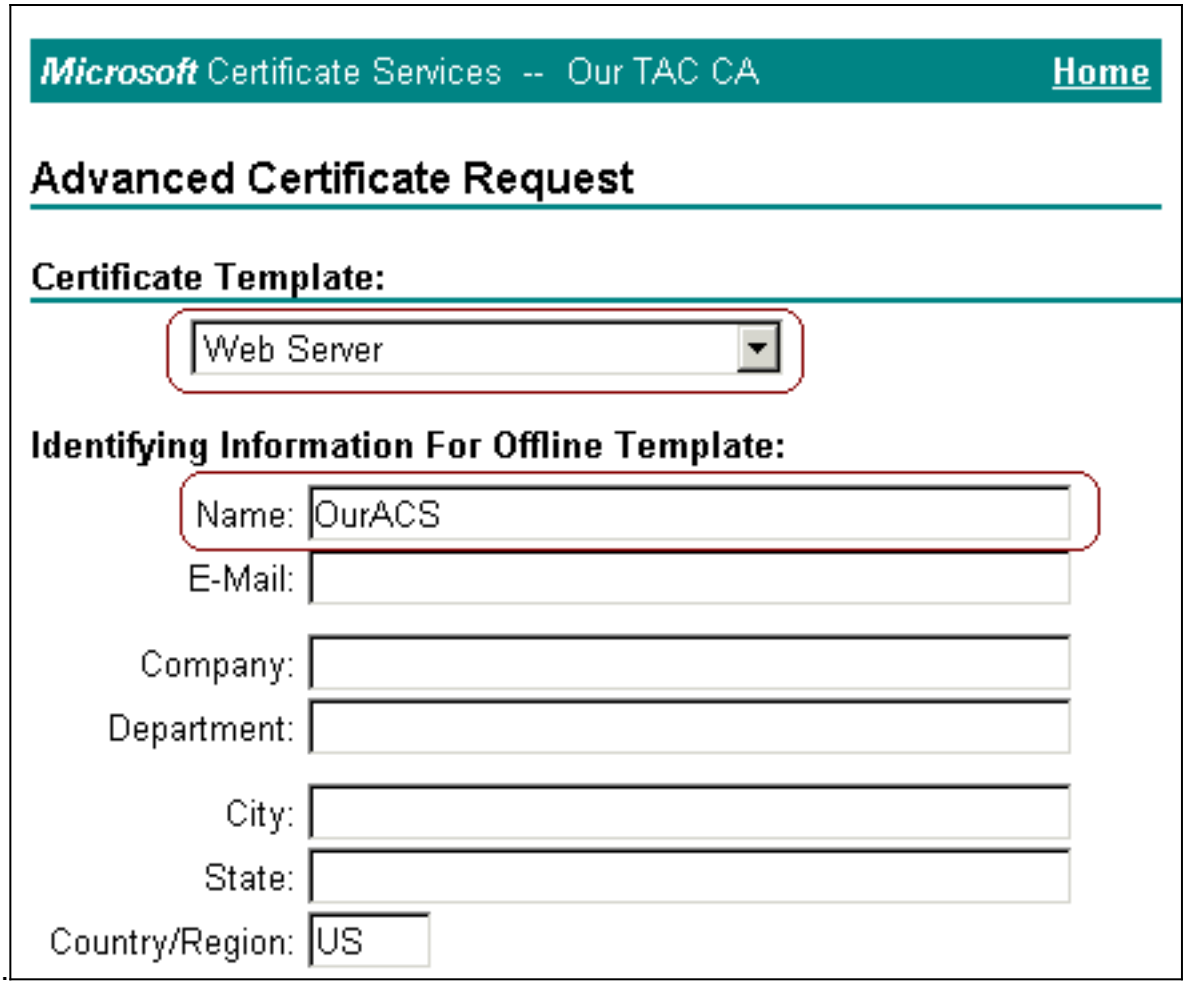

(Далее).

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



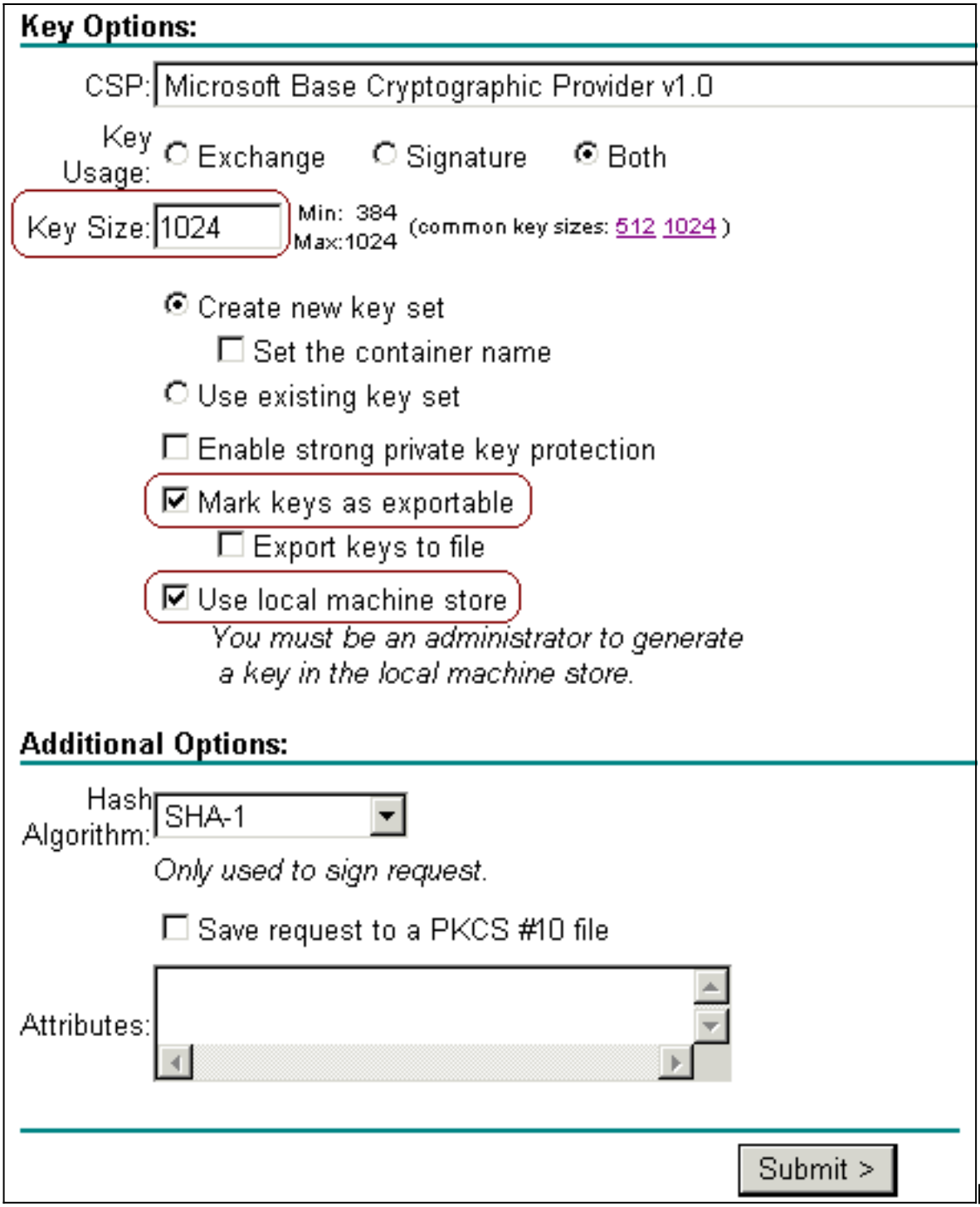

**(Далее).**

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



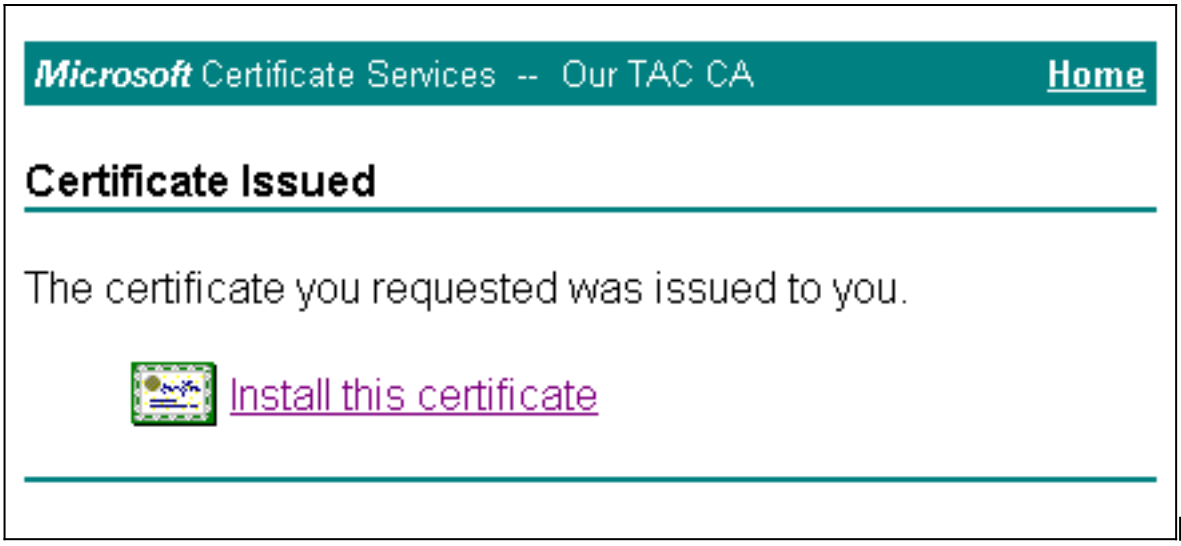

сервера.

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.

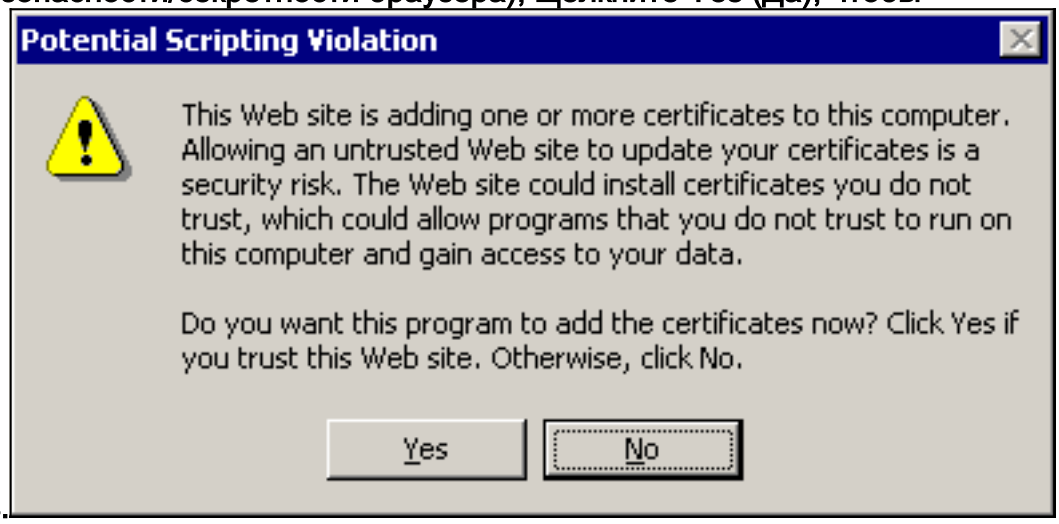



Примечание: Если появится окно предупреждения о нарушении сценария (в зависимости от настроек безопасности/секретности браузера), щелкните Yes (Да), чтобы продолжить.

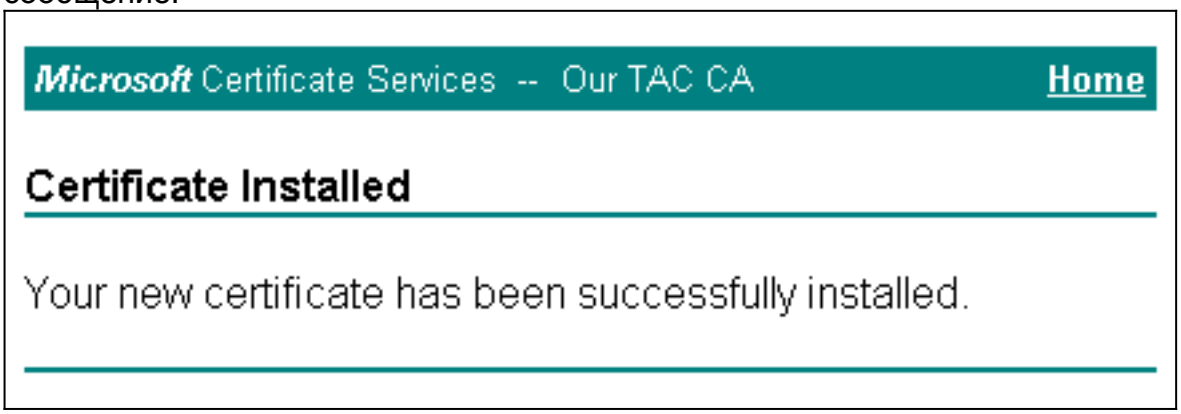

6. Нажмите кнопку Install this certificate (Установить этот сертификат).




**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.

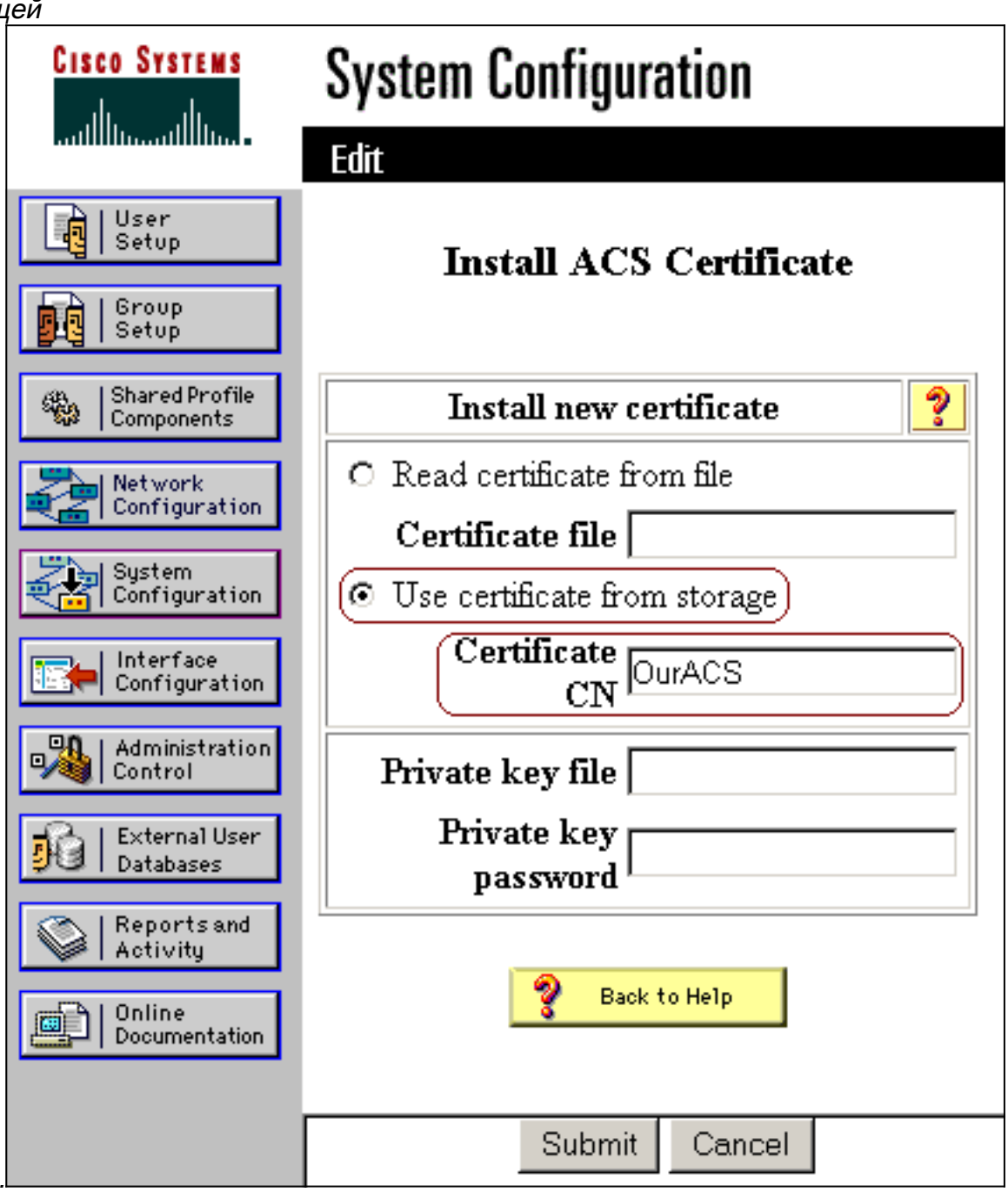



## Настройте ACS для использования сертификата из хранилища

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).**

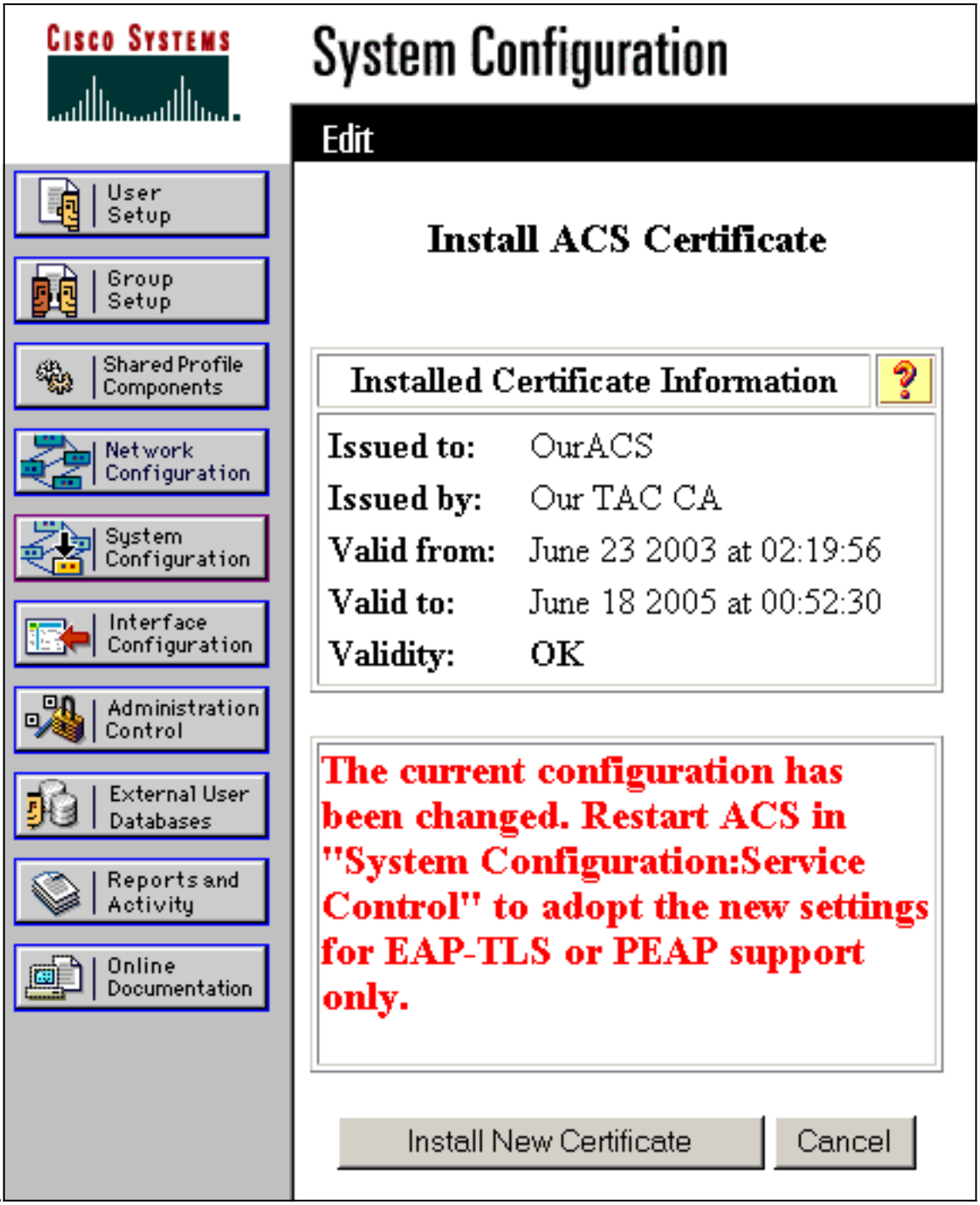
3. **Выберите вариант использования сертификата из хранилища.** В поле Certificate CN введите имя сертификата, который вы назначили в шаге 5a раздела, Получают Сертификат для Сервера ACS. **Нажмите кнопку Submit (Отправить).**Эта запись должна совпадать с именем, введенным в поле "Name" во время расширенного 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*




*службы.*

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

требуется.




## Указание дополнительных CA, 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 CA и нажмите кнопку Submit (Отправить).


3. **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).**


## 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 AuthenticationПримечание:** Дополнительную информацию по функции быстрого установления соединения Fast Connect см. в подразделе "Параметры конфигурации аутентификации" раздела "Конфигурация системы": Проверка подлинности и сертификаты.