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

Содержание

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 компьютеровРуководства пользователя сервера управления доступом Cisco 4.1.

Примечание: Когда устанавливание 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

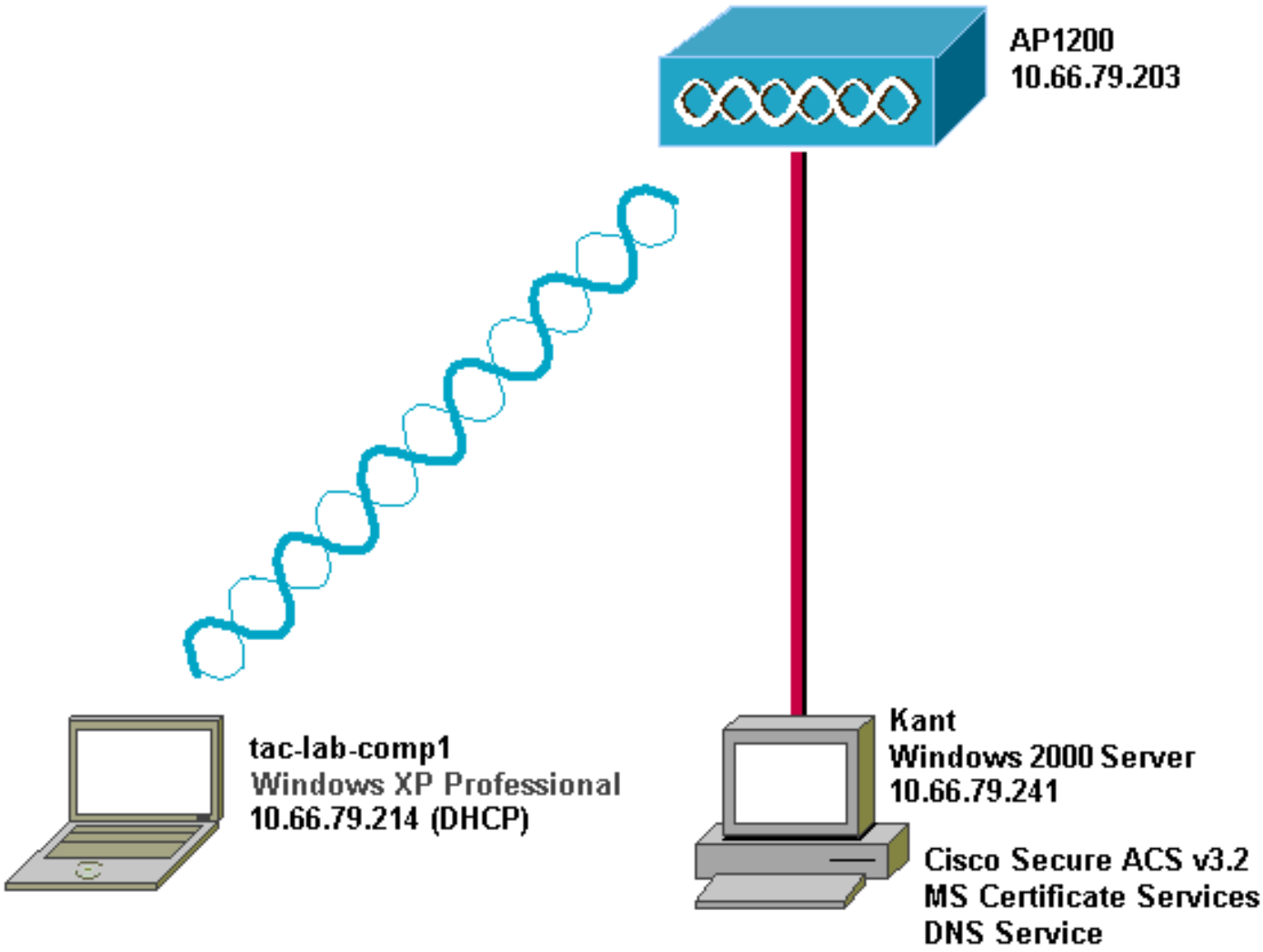
И EAP-TLS, и защищенный расширяемый протокол аутентификации (PEAP) образуют и используют туннель TLS/Secure Socket Layer (SSL). EAP-TLS использует взаимную аутентификацию, при которой сервер управления доступом (AAA) и клиенты имеют сертификаты и удостоверяют личности друг друга. В то же время, PEAP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

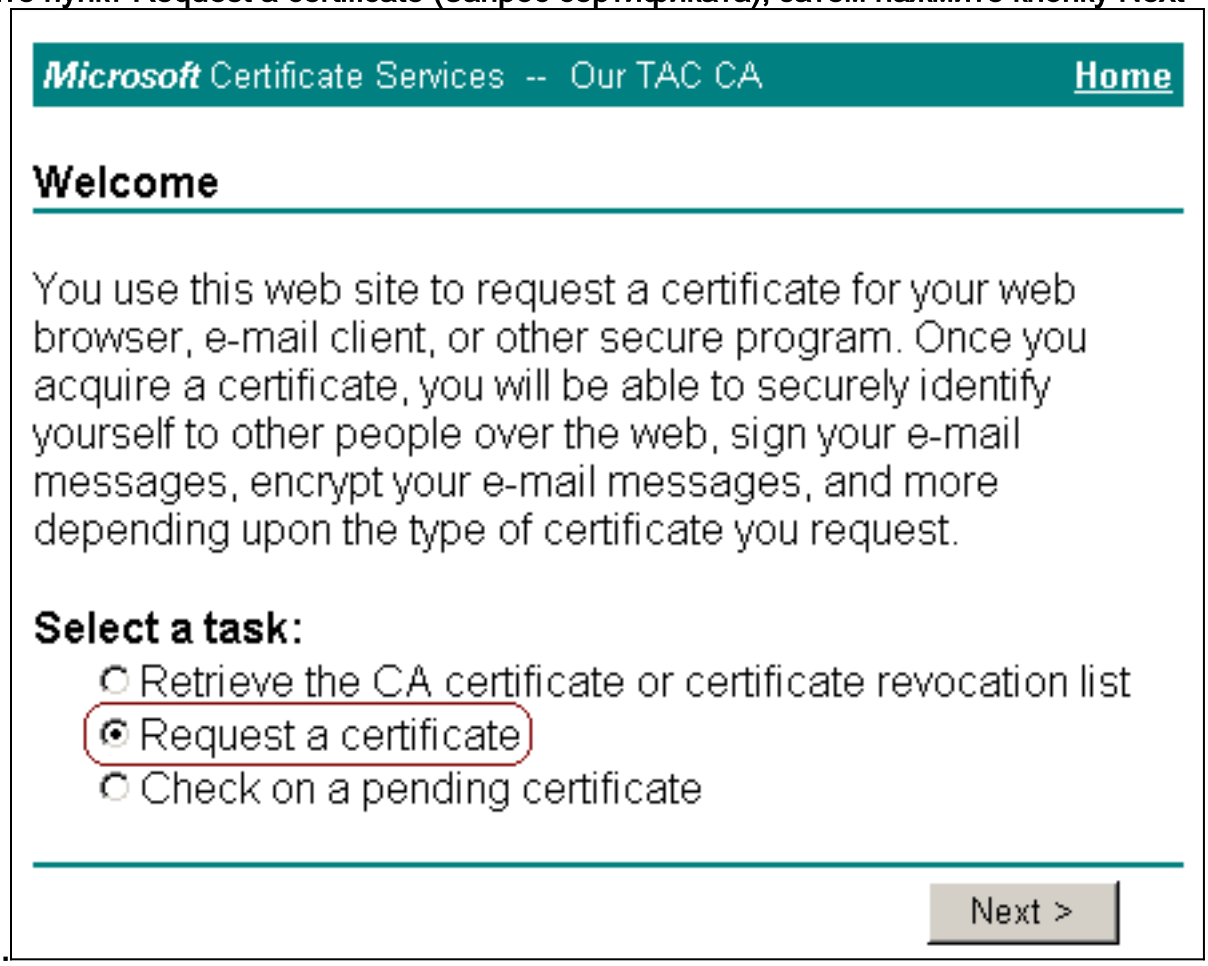
Получение сертификата для сервера ACS

Чтобы получить сертификат, выполните данные шаги.

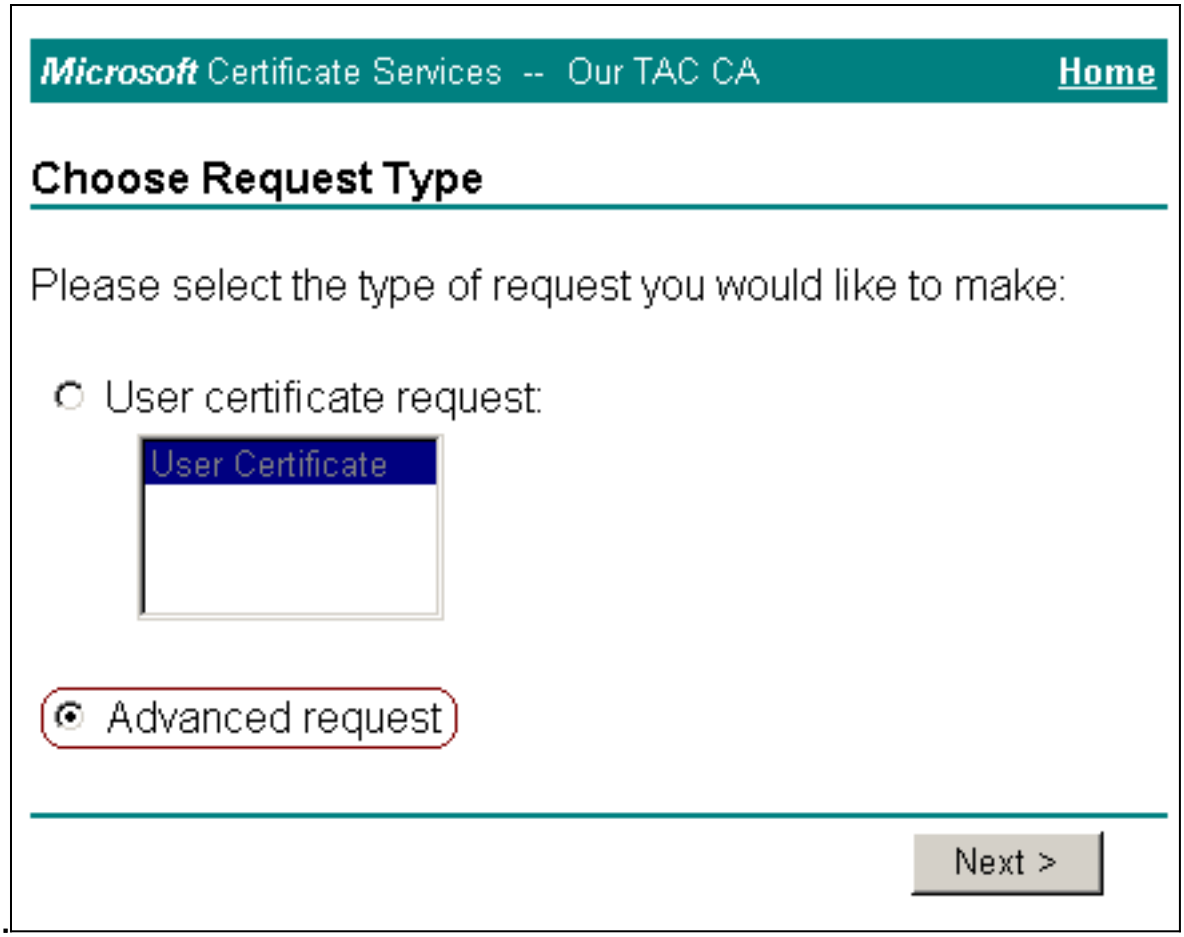
1. *На сервере ACS отройте браузер и войдите на сервер центра сертификации, набрав адрес http://ip-адрес-центра-сертификации/certsrv.*

2. Войдите в домен с правами администратора.

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

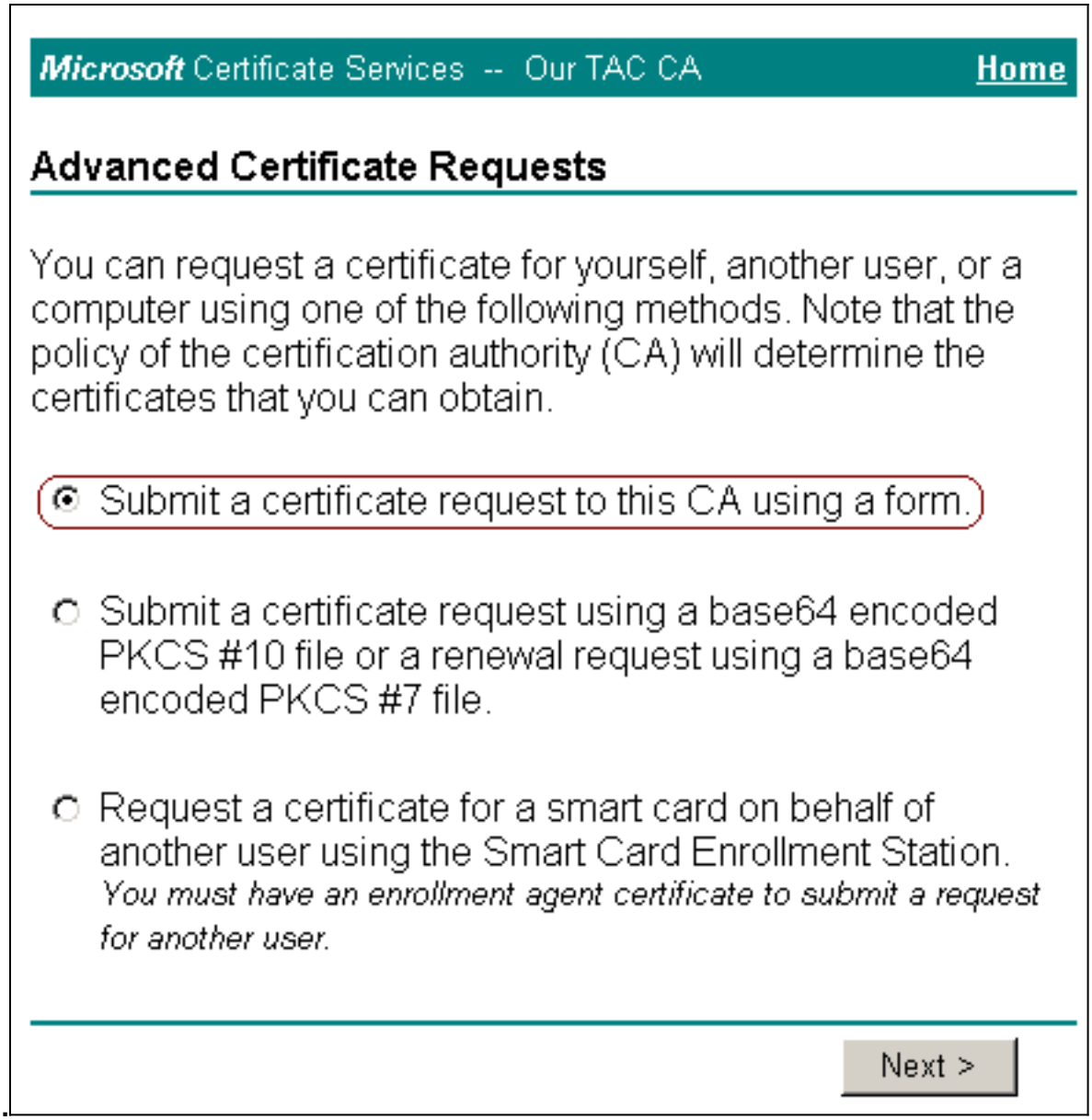


4. **Выберите Advanced request (Расширенный запрос) и нажмите кнопку Next**



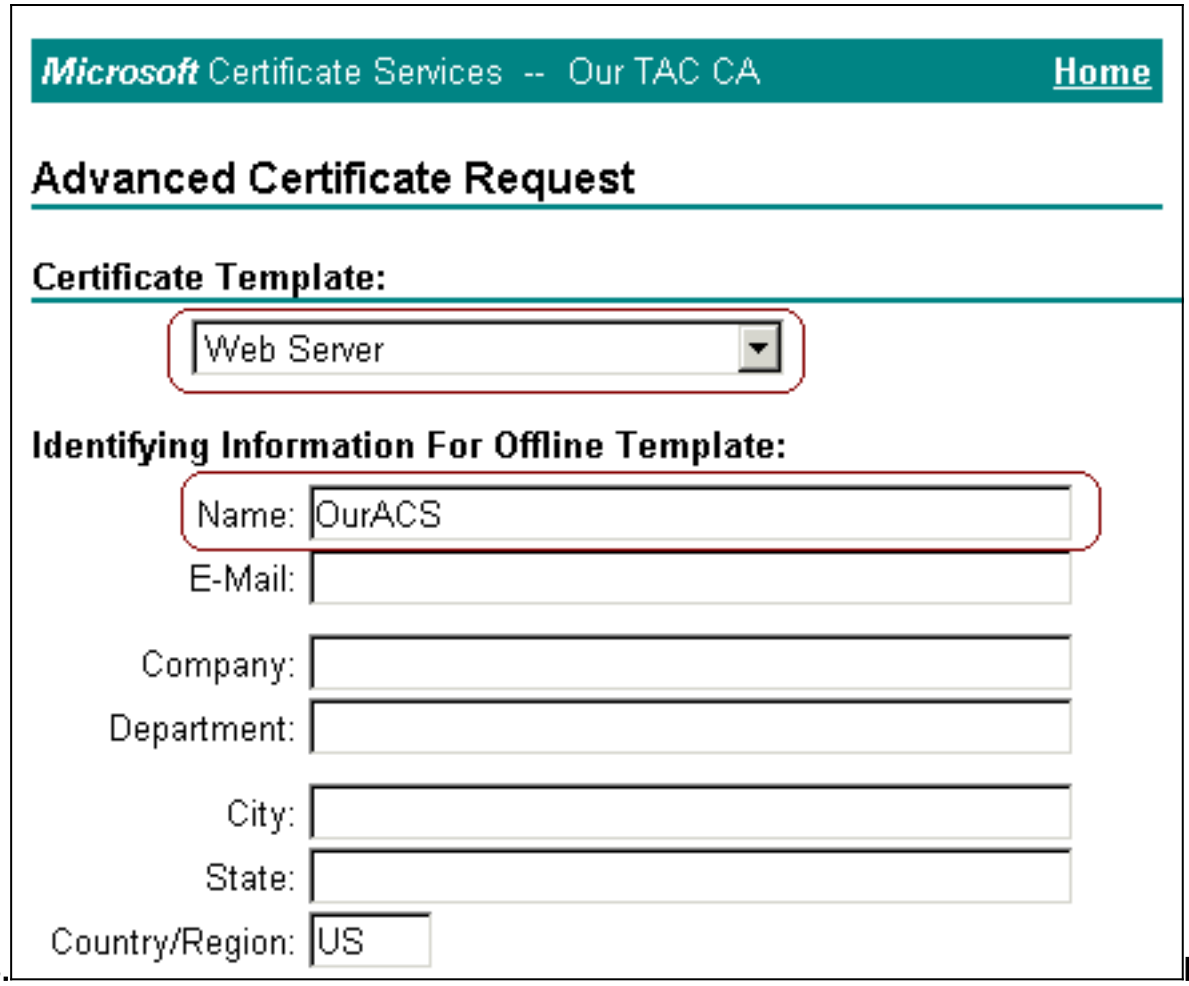
(Далее).

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

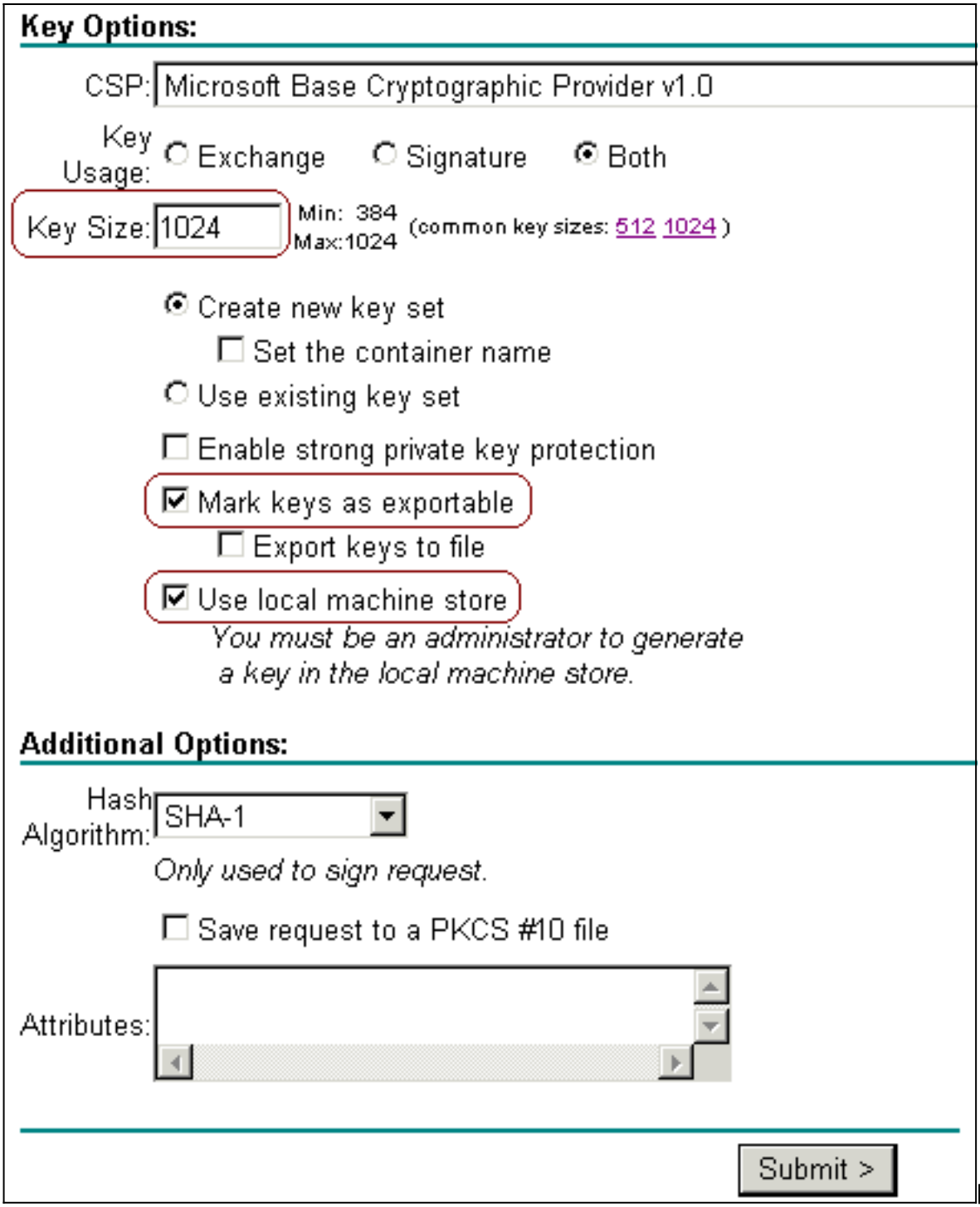


(Далее).

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

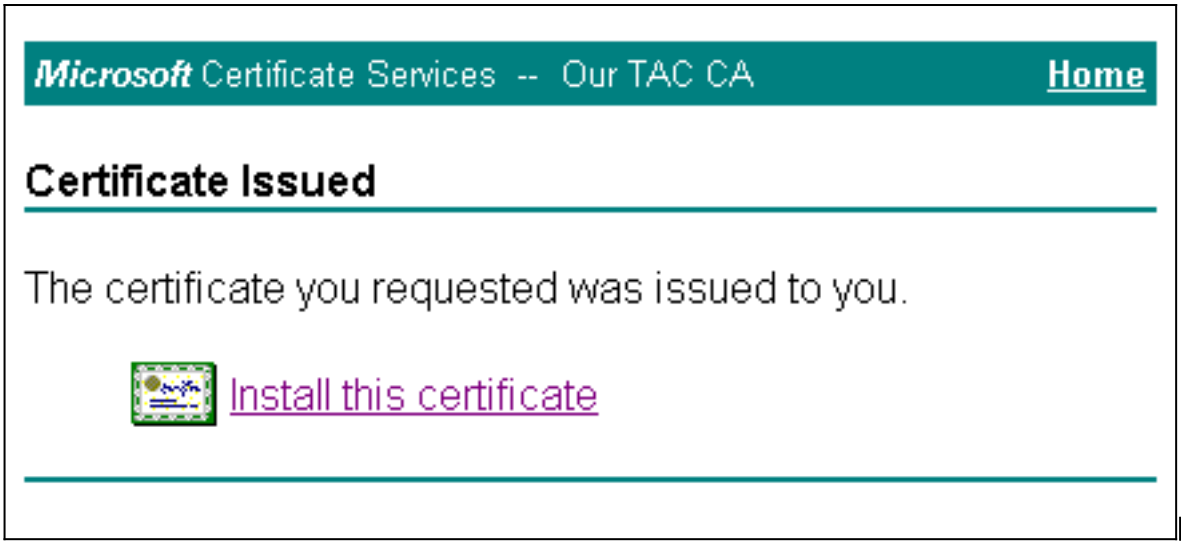


ACS. В поле Key Size (Размер ключа) введите 1024, затем отметьте флажки Mark keys as exportable (Пометить ключи как экспортируемые) и Use local machine store (Использовать локальное хранилище компьютера).Настройте остальные параметры необходимым образом и нажмите кнопку Подтвердить.

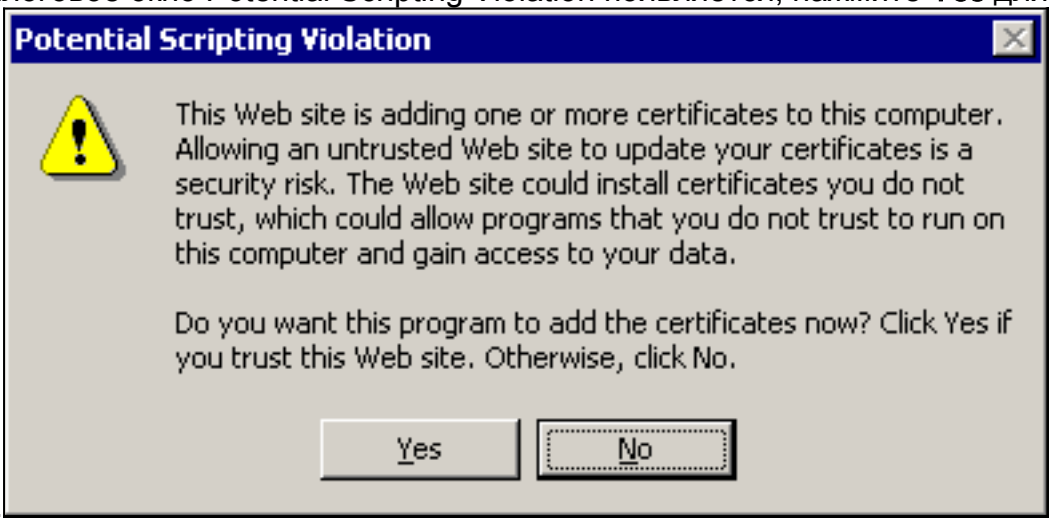


Примечание: Если диалоговое окно Potential Scripting Violation появляется, нажмите **Yes** для продолжения.

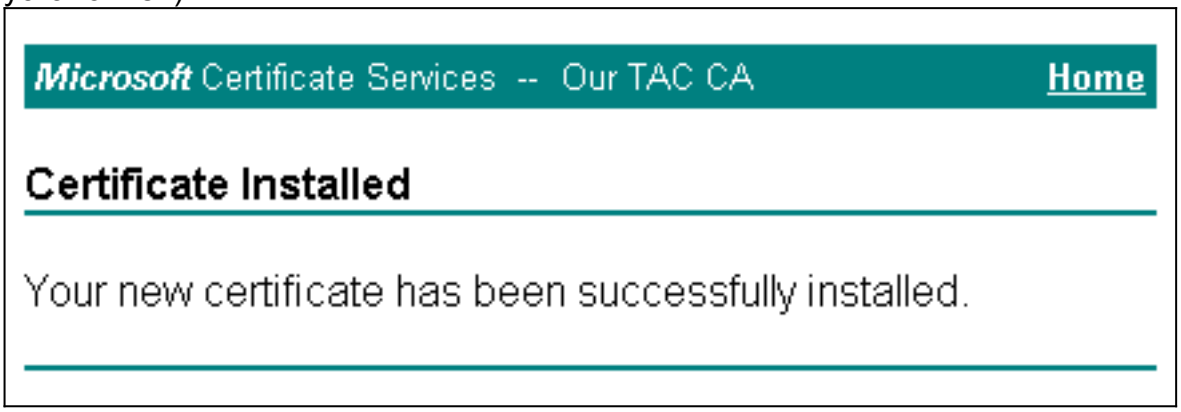
7. **Нажмите кнопку Install this certificate (Установить этот сертификат).**



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



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

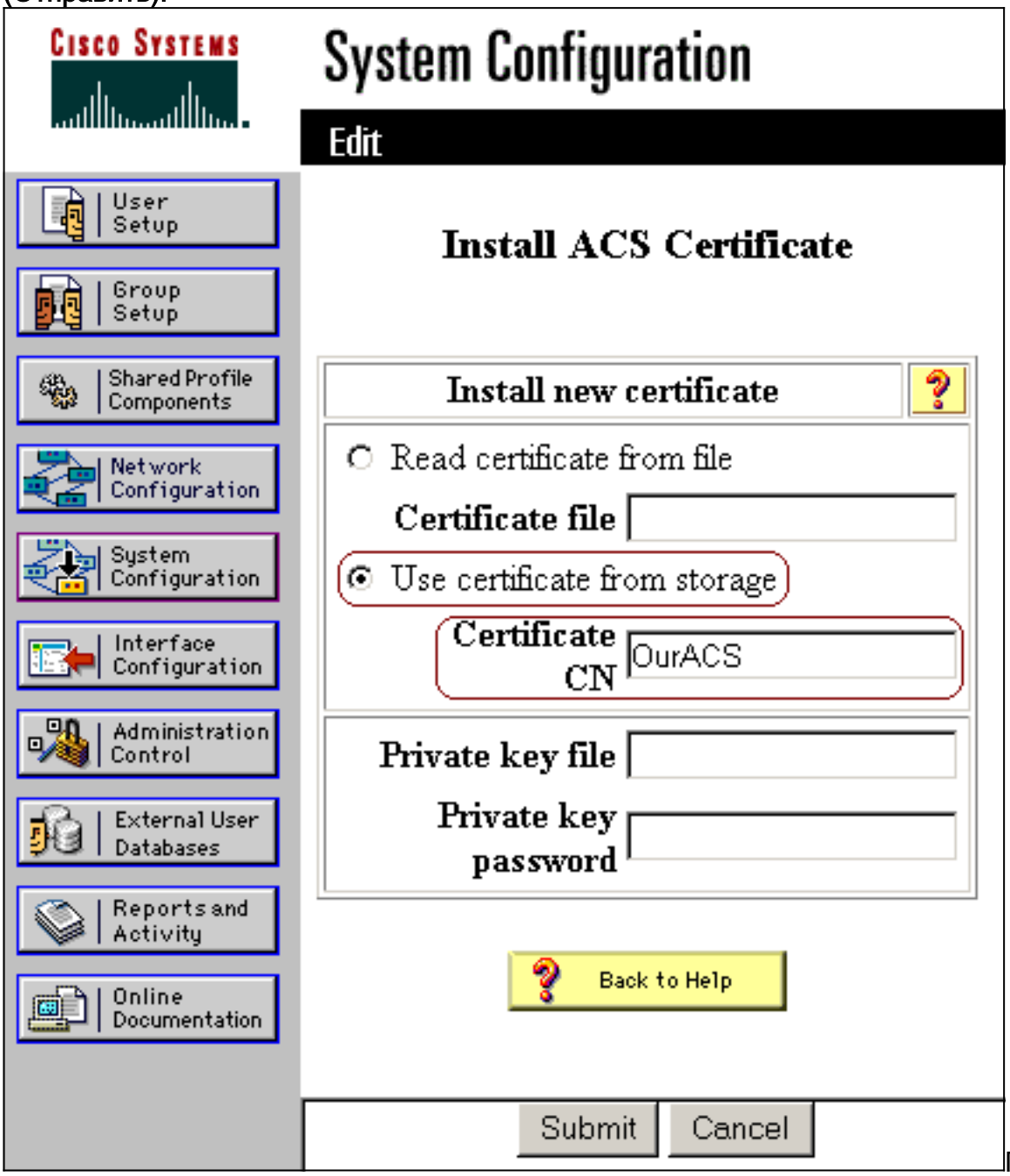


Настройте ACS для использования сертификата из хранилища

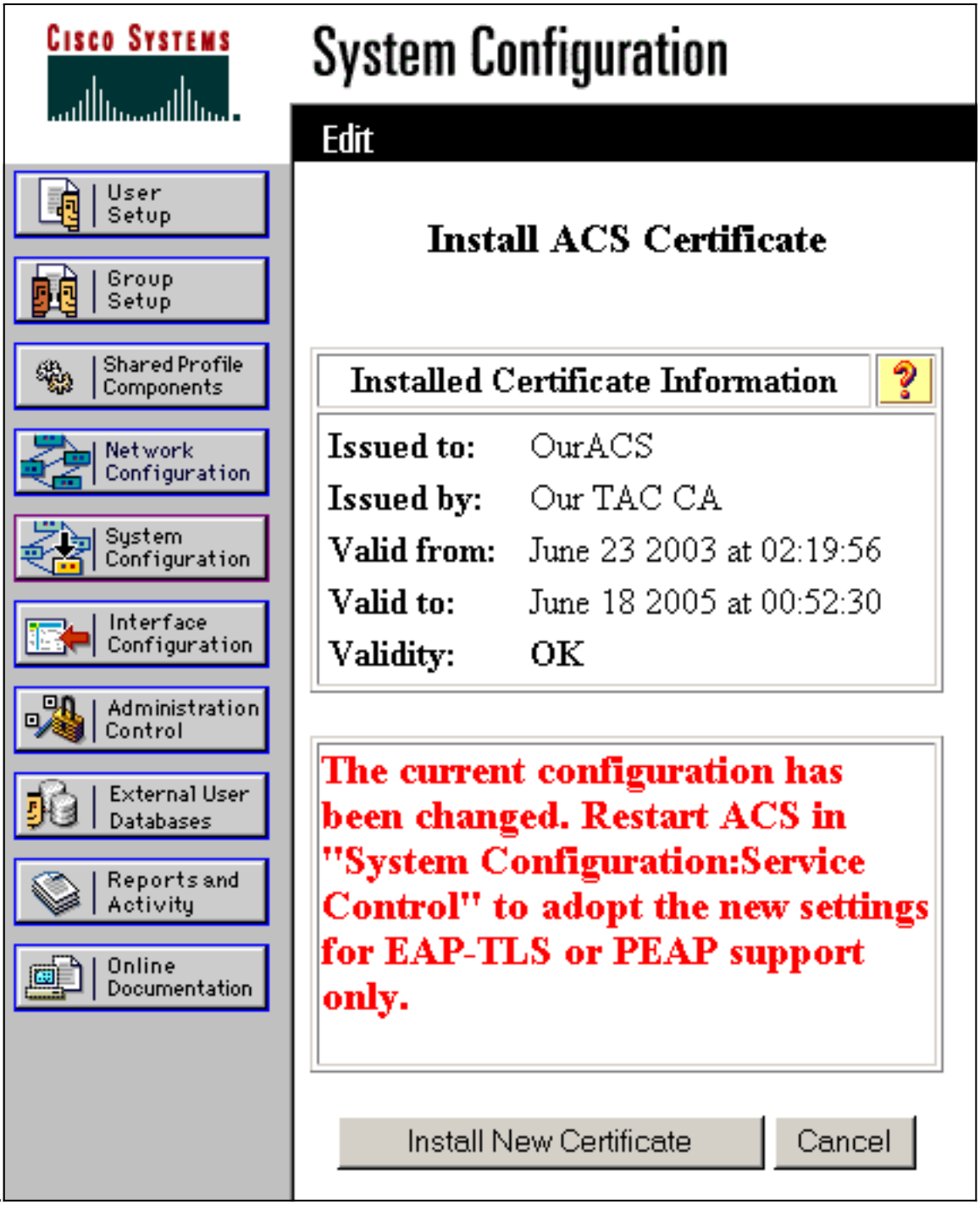
Чтобы настроить ACS для использования сертификата из хранилища, выполните следующие действия.

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 5a раздела Получение сертификата от сервера ACS настоящего документа.
6. **Нажмите кнопку Submit (Отправить).**



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 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 CA и нажмите кнопку Submit
(Отправить).

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).**

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).