ASA 8. x: Возобновление и установка SSL-сертификата с помощью ASDM

Содержание

Введение

Процедура в этом документе является примером и может использоваться в качестве рекомендации с любым поставщиком сертификата или вашим собственным сервером корневого сертификата. Специальные требования параметра сертификата иногда требуются вашим поставщиком сертификата, но этот документ предназначен для обеспечения общих действий, требуемых возобновить сертификат SSL и установить его на ASA, который использует 8.0 программных обеспечений.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Эта процедура принадлежит версиям ASA 8.x с версией 6.0 (2) ASDM или позже.

Процедура в этом документе основывается на допустимой конфигурации с сертификатом, установленным и используемым для доступа VPN SSL. Эта процедура не влияет на вашу сеть, пока не удален текущий сертификат. Эта процедура является пошаговым процессом о том, как выполнить новый CSR для текущего сертификата с тем же корневым сертификатом, который выполнил исходный узел CA.

Сведения, представленные в этом документе, были получены от устройств, работающих в

специальной лабораторной среде. Если используемая сеть является действующей, убедитесь в понимании возможного влияния любой из применяемых команд.

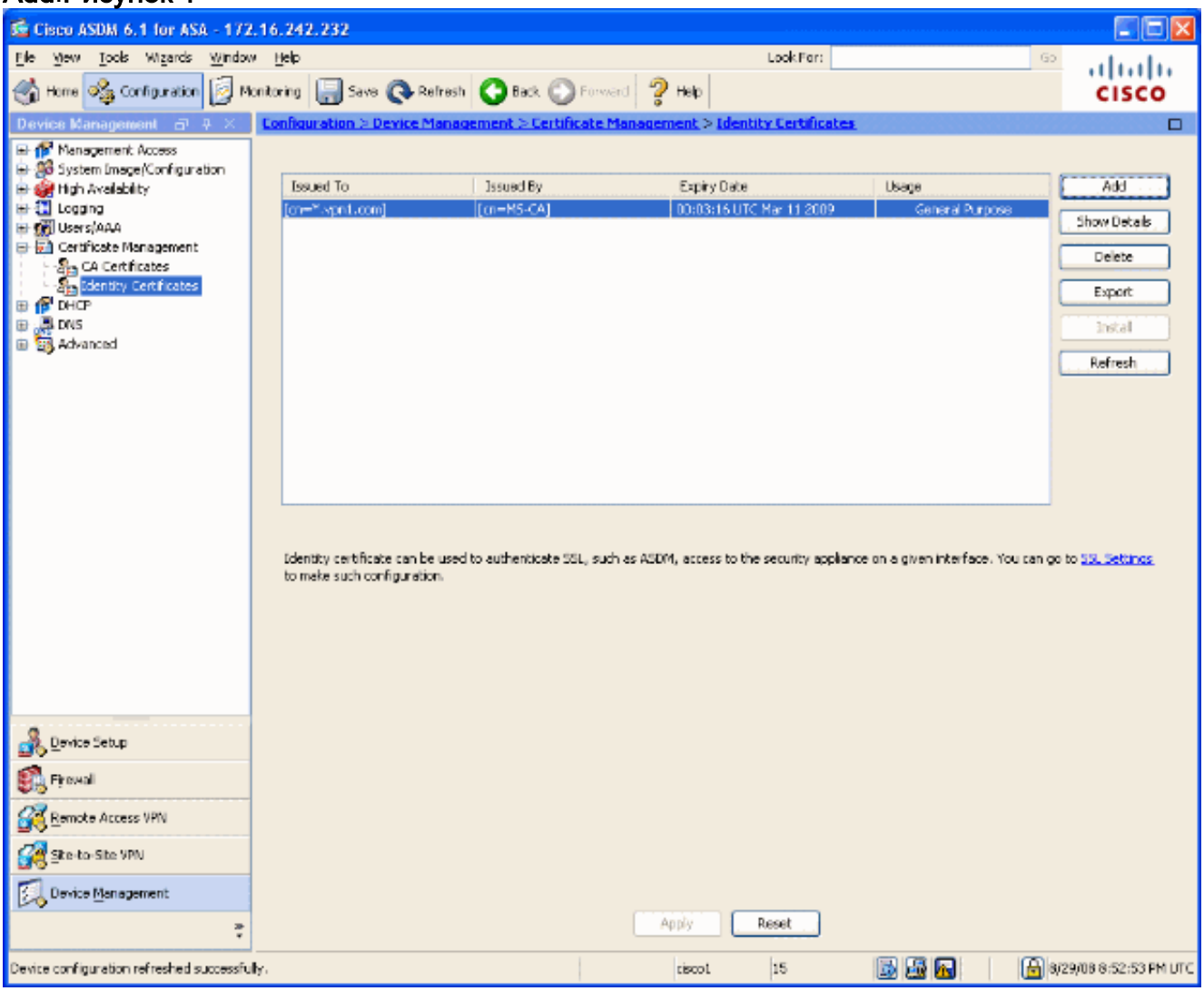
Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

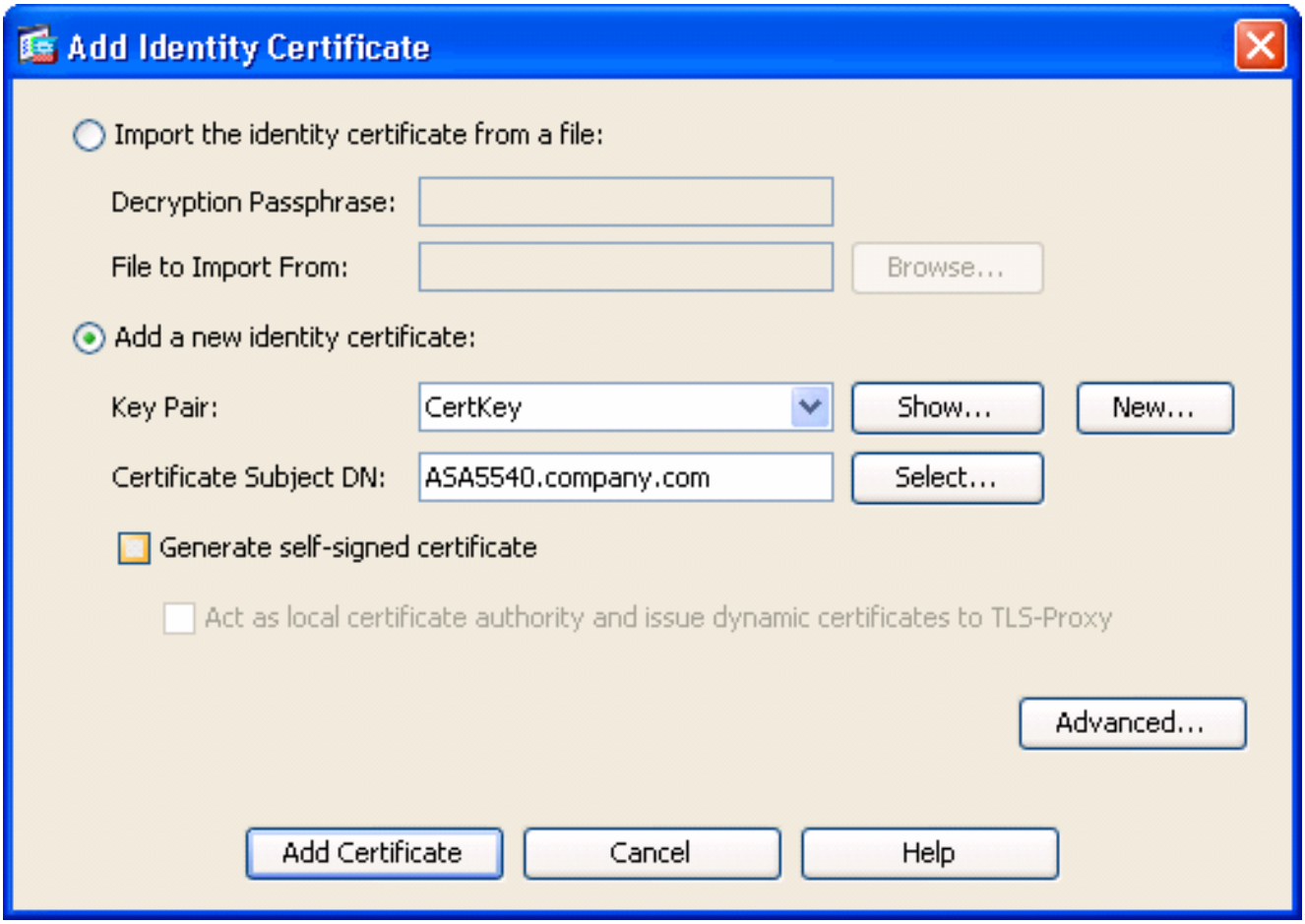
Процедура

Выполните следующие действия:

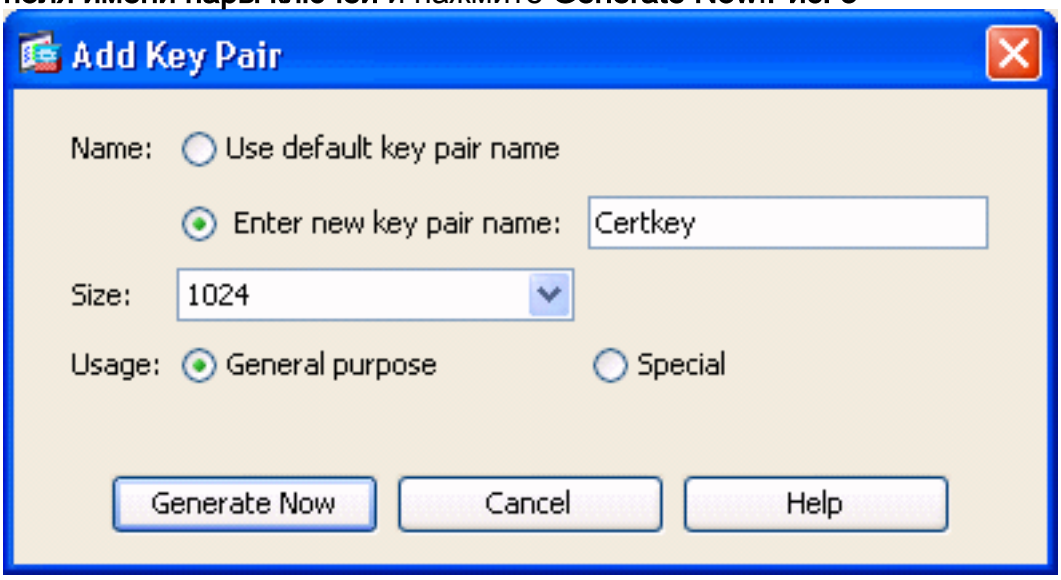
1. Выберите сертификат, который вы хотите возобновить ниже Конфигурации> Управление устройствами> Сертификаты идентификации, и затем **нажмите Add.Рисунок 1**



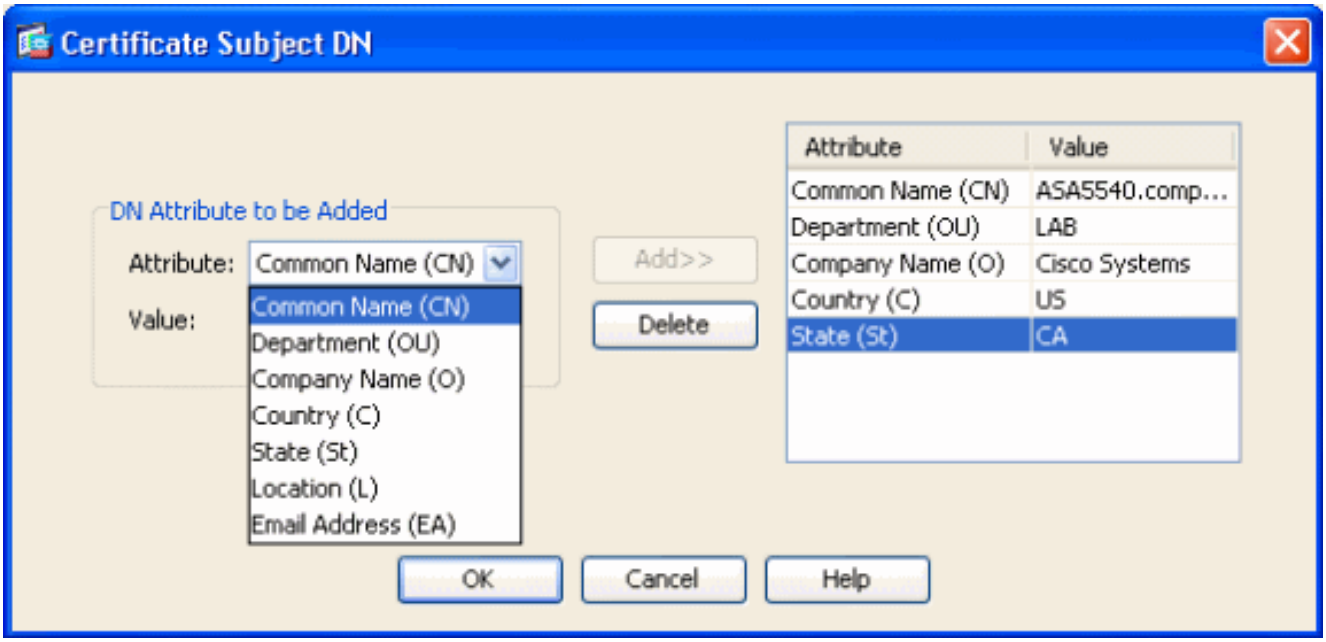
2. Под Добавляют Сертификат идентификации, выбирают **Add новая** кнопка с зависимой фиксацией **сертификата идентификации** и выбирают вашу пару ключей из раскрывающегося меню.**Примечание:** Не рекомендуется использовать <Ключ RSA по умолчанию>, потому что при регенерации SSH-ключа вы лишаете законной силы свой сертификат. Если у вас нет ключа RSA, выполните Шаги и b. Иначе перейдите к шагу 3.**Рис. 2**



(Необязательно) Выполните эти шаги, если вам еще не настроили ключ RSA, иначе пропустите к Шагу 3.**Щелкните New...**.Введите имя пары ключей во **Введении нового поля имени пары ключей** и нажмите **Generate Now**.**Рис. 3**



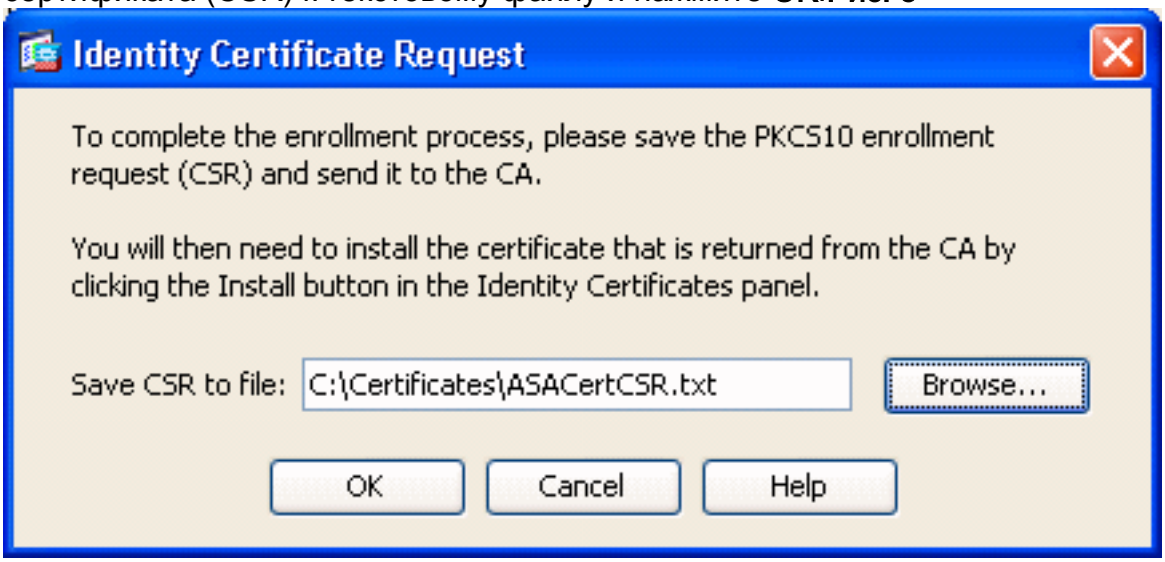
3. Нажмите **Select**.
4. Введите соответствующие атрибуты сертификата как показано в рисунок 4. После того, как завершенный, нажмите **OK**. Затем **нажмите Add Сертификат**.**Рис. 4**



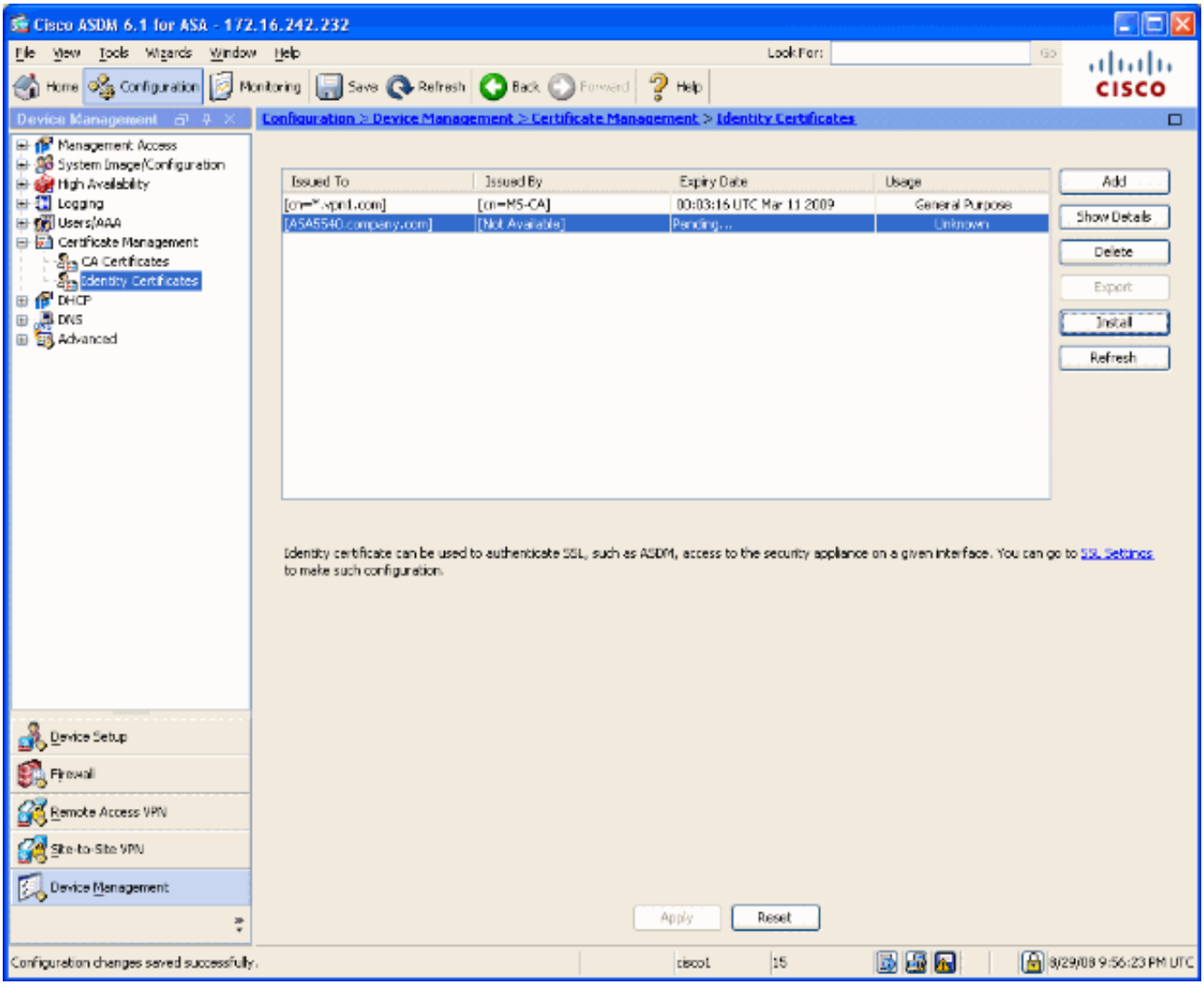
Выходные данные CLI:

```
crypto ca trustpoint ASDM_TrustPoint0 keypair CertKey id-usage ssl-ipsec fqdn 5540-uwe
subject-name CN=ASA5540.company.com,OU=LAB,O=Cisco ystems,C=US,St=CA enrollment terminal
crypto ca enroll ASDM_TrustPoint0
```

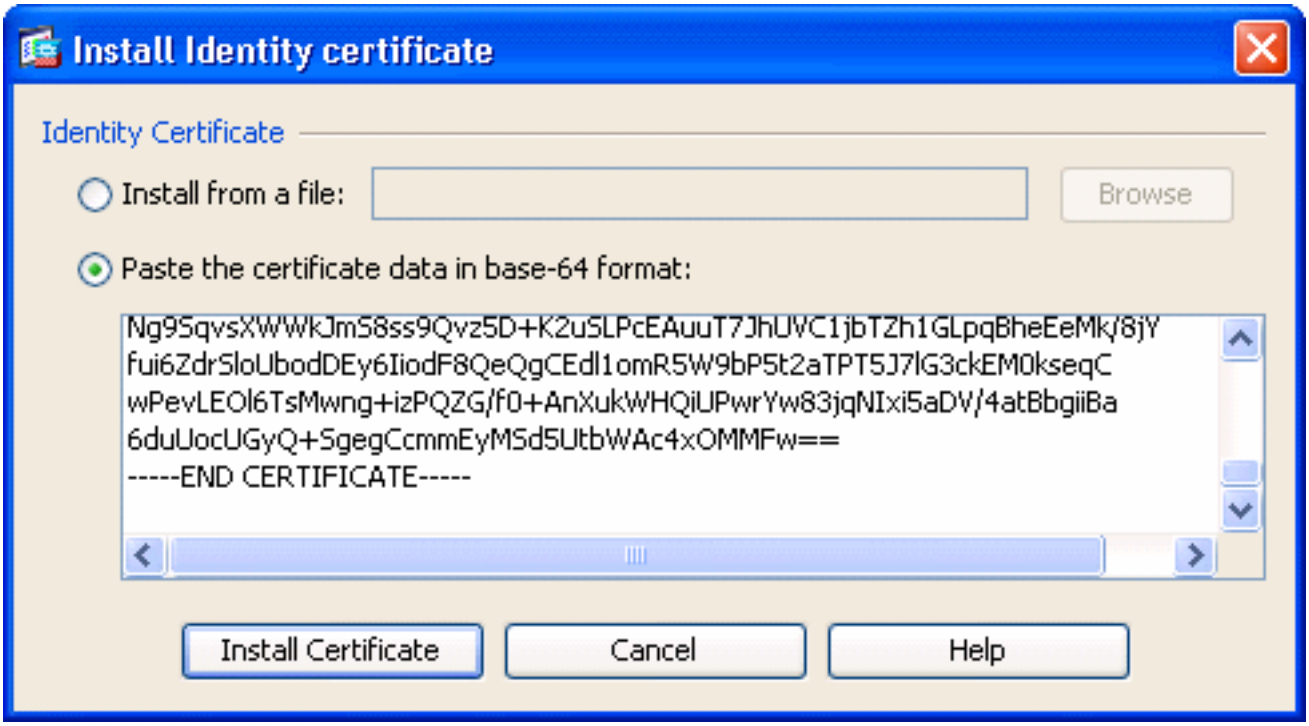
5. Во всплывающем окне **Identity Certificate Request** сохраните свой Запрос подписи сертификата (CSR) к текстовому файлу и нажмите **OK**.**Рис. 5**



6. (Необязательно) Проверьте в ASDM, что CSR находится на рассмотрении, как показано на рисунке 6.**Рис. 6**



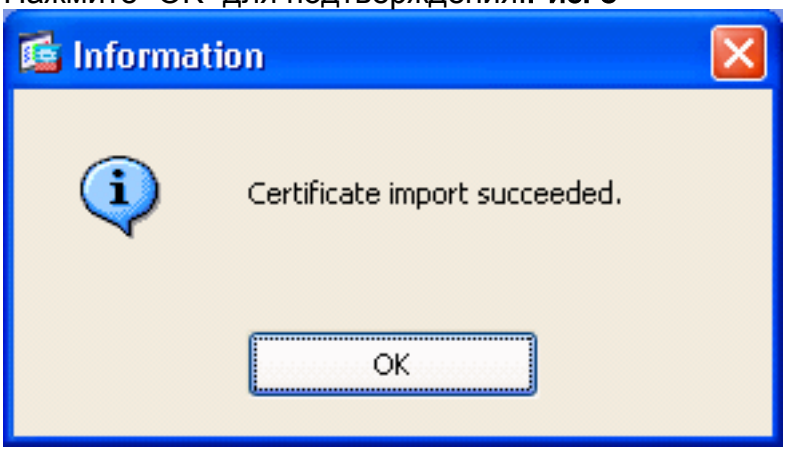
7. Отправьте запрос сертификата администратору сертификата, который выполняет сертификат на сервере. Это может или быть через веб-интерфейс, электронную почту, или непосредственно к серверу узла CA для процесса проблемы сертификата.
8. Выполните эти шаги для установки возобновленного сертификата.Выберите запрос сертификата в состоянии ожидания под Конфигурацией> Управление устройствами> Сертификаты идентификации, как показано на рисунке 6, и нажмите **Install**.В окне Install Identity Certificate выберите **Paste данные сертификата в** кнопке с зависимой фиксацией **формата base64** и нажмите **Install Certificate**.**Примечание:** Также, если сертификат выполнен в .cer файле скорее тогда, текст базировал файл или электронную почту, можно также выбрать **Install от файла**, перейти к соответствующему файлу на ПК, нажать **файл сертификата Install ID** и затем нажать **Install Certificate**.**Рисунок 7**



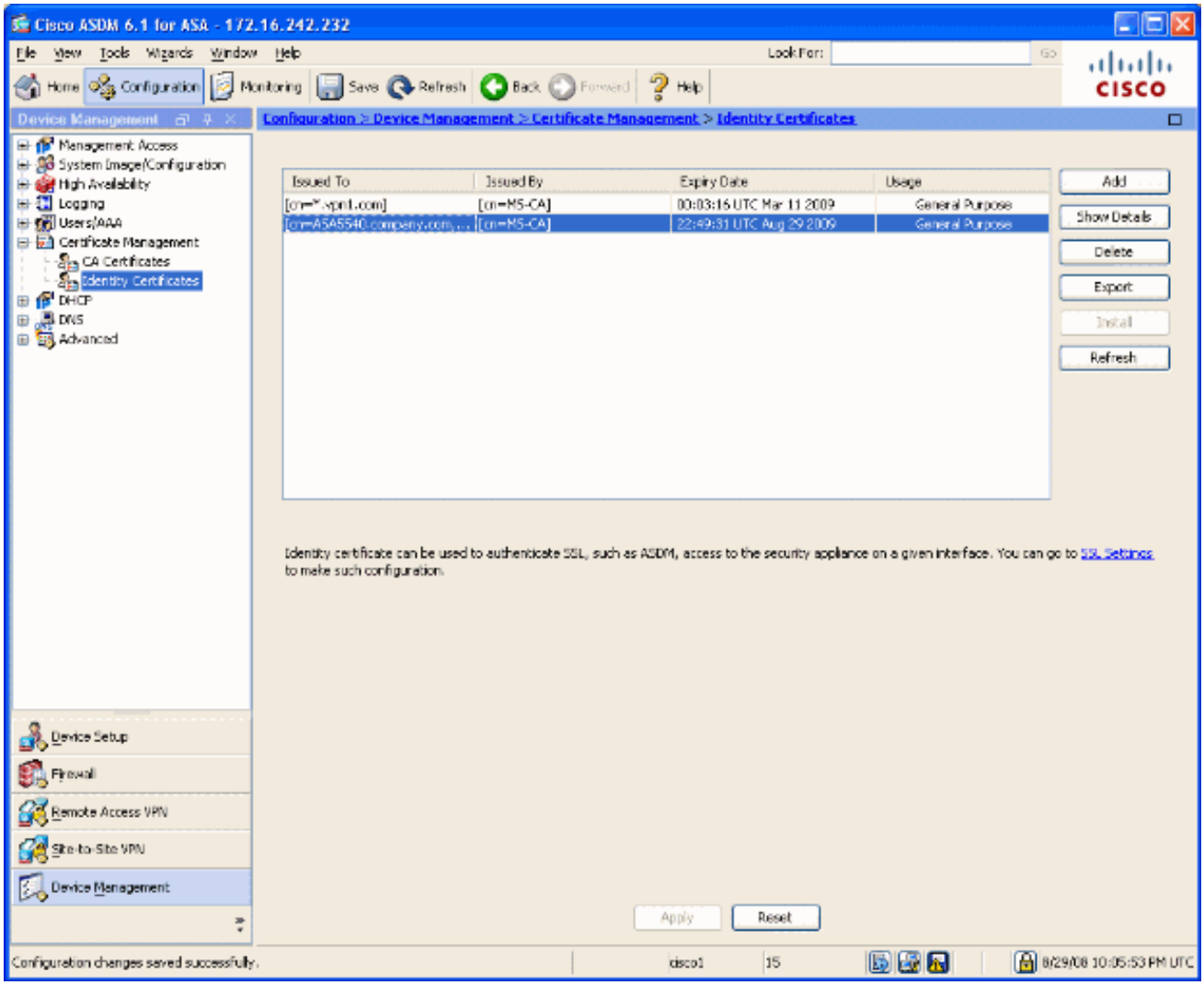
Выходные данные CLI:

```
crypto ca import ASDM_TrustPoint0 certificate
WIID2DCCAsCgAwIBAgIKYb9wewAAAAAAJzANBgkqhkiG9w0BAQUFADAQMQ !--- output truncated
wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa
6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== quit
```

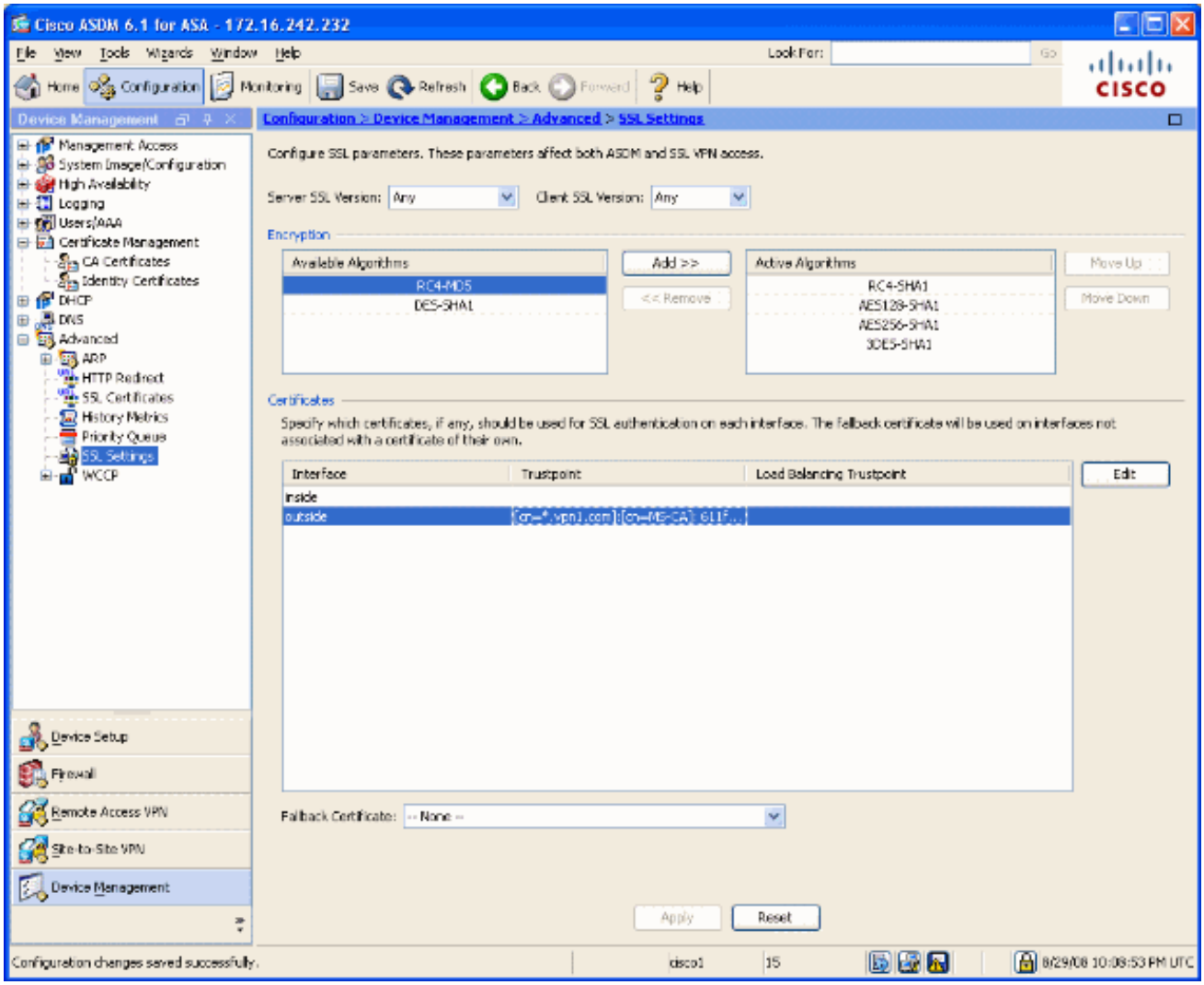
9. Окно появляется, который подтверждает, что успешно установлен сертификат. Нажмите “OK” для подтверждения.**Рис. 8**



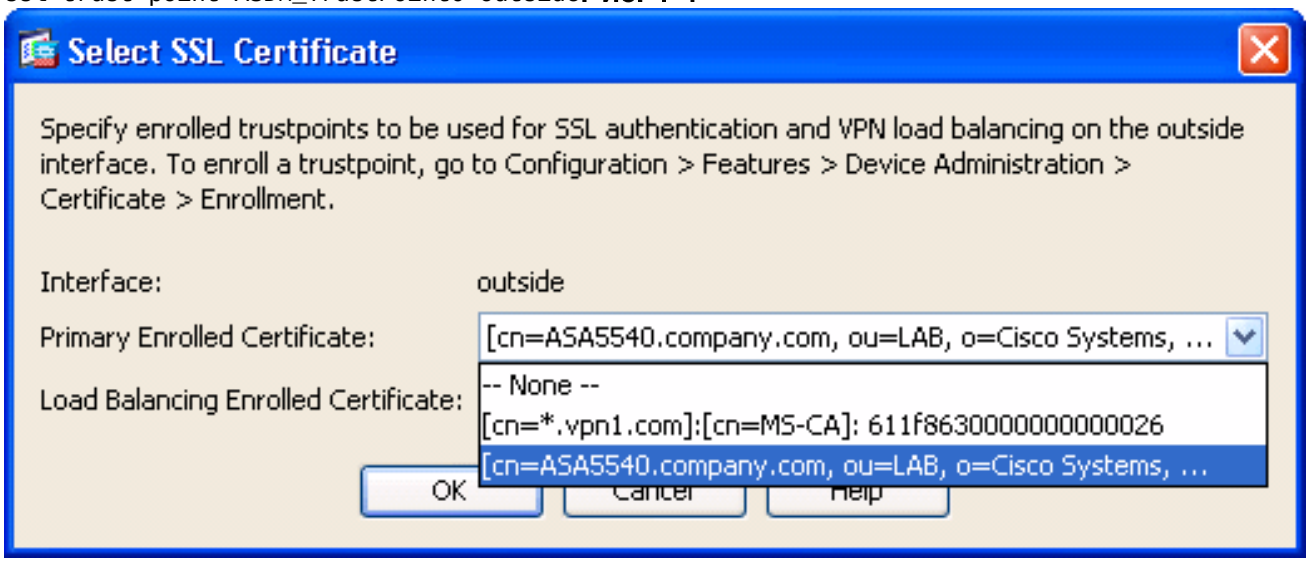
10. Гарантируйте, что ваш новый сертификат появляется под Сертификатами идентификации.**Рис. 9**



11. Выполните эти шаги для привязки нового сертификата с интерфейсом:Выберите **Configuration> Device Management> Advanced> SSL Settings**, как показано на рисунке 10.Выберите свой интерфейс под Сертификатами и нажмите **Edit**.**Рис. 10**



12. Выберите свой новый сертификат из раскрывающегося меню, **нажмите OK** и нажмите **Apply**.`ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1`
`ssl trust-point ASDM_TrustPoint0 outside`**Рис. 1-1**



13. Сохраните свою конфигурацию или в ASDM или на CLI.

Проверка

Можно использовать CLI - интерфейс, чтобы проверить, что новый сертификат установлен к ASA правильно, как показано в этом примере выходных данных:

```
ASA(config)#show crypto ca certificates Certificate Status: Available Certificate Serial Number:
61bf707b000000000027 Certificate Usage: General Purpose Public Key Type: RSA (1024 bits) Issuer
Name: cn=MS-CA Subject Name: cn=ASA5540.company.com !---new certificate ou=LAB o=Cisco Systems
st=CA c=US CRL Distribution Points: [1] http://win2k3-base1/CertEnroll/MS-CA.crl [2]
file://\\win2k3-base1\CertEnroll\MS-CA.crl Validity Date: start date: 22:39:31 UTC Aug 29 2008
end date: 22:49:31 UTC Aug 29 2009 Associated Trustpoints: ASDM_TrustPoint0 CA Certificate
Status: Available Certificate Serial Number: 211020a79cfd96b34ba93f3145d8e571 Certificate Usage:
Signature Public Key Type: RSA (2048 bits) Issuer Name: cn=MS-CA Subject Name: cn=MS-CA !---
'old' certificate CRL Distribution Points: [1] http://win2k3-base1/CertEnroll/MS-CA.crl [2]
file://\\win2k3-base1\CertEnroll\MS-CA.crl Validity Date: start date: 00:26:08 UTC Jun 8 2006
end date: 00:34:01 UTC Jun 8 2011 Associated Trustpoints: test Certificate Status: Available
Certificate Serial Number: 611f8630000000000026 Certificate Usage: General Purpose Public Key
Type: RSA (1024 bits) Issuer Name: cn=MS-CA Subject Name: cn=*.vpn1.com CRL Distribution Points:
[1] http://win2k3-base1/CertEnroll/MS-CA.crl [2] file://\\win2k3-base1\CertEnroll\MS-CA.crl
Validity Date: start date: 23:53:16 UTC Mar 10 2008 end date: 00:03:16 UTC Mar 11 2009
Associated Trustpoints: test ASA(config)#
```

Устранение неполадок

(Необязательно) Проверьте на CLI, что корректный сертификат применен к интерфейсу:

```
ASA(config)#show running-config ssl ssl trust-point ASDM_TrustPoint0 outside !--- Shows that the
correct trustpoint is tied to the outside interface that terminates SSL VPN. ASA(config)#
```

Как скопировать сертификаты SSL от одного ASA до другого

Это может быть сделано при генерации экспортных ключей. Необходимо экспортировать сертификат в файл PKCS. Это включает экспортирование всех связанных ключей.

Используйте эту команду для экспортирования сертификата через CLI:

```
ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>
```

Примечание: Парольная фраза - использовала защищать файл pkcs12.

Используйте эту команду для импорта сертификата через CLI:

```
SA(config)#crypto ca import <trust-point-name> pkcs12 <passphrase>
```

Примечание: Этот пароль должен совпасть с используемый при экспортировании файла.

Это может также быть сделано через ASDM для пары аварийного переключения ASA. Выполните эти шаги для выполнения этого:

1. Вход в систему к основному ASA через ASDM и выбирает **Tools-> Backup Configuration**.
2. Можно резервировать все или просто сертификаты.
3. На резерве откройте ASDM и выберите **Tools-> Restore Configuration**.

Дополнительные сведения

- Устройство адаптивной защиты Cisco (ASA) страница технической поддержки
- ASA 8. x Вручную Сертификаты Поставщика третьей стороны Установки для использования с Примером конфигурации WebVPN
- Cisco Systems – техническая поддержка и документация