

Создание сертификата ESA для использования с подписанием S/MIME

Содержание

[Введение](#)

[Общие сведения](#)

[Создайте сертификат](#)

[Импортируйте сертификат](#)

[Привяжите сертификат PEM](#)

[Дополнительные сведения](#)

Введение

Этот документ описывает, как создать сертификаты для использования с Безопасными / Многоцелевыми расширениями почты в Интернете (S/MIME) , подписывающийся на Cisco Email Security Appliance (ESA).

Общие сведения

При создании сертификата S/MIME для подписания сообщения это должно удовлетворить требования, описанные в [RFC 5750](#): Безопасные / Многоцелевые расширения почты в Интернете (S/MIME) Версия 3.2 - Обработка Сертификата.

Для этого процесса использование внешнего приложения требуется для генерации сертификата. X Сертификатов и Управление ключами (XCA) являются приложением , которое управляет асимметричными ключами, такими как алгоритм цифровой подписи райвеста шамира адлемана (RSA) или Алгоритм цифровой подписи (DSA), и предназначено, чтобы быть маленьким Центром сертификации (CA) для создания и подписания сертификатов. Это пользуется библиотекой Open Secure Sockets Layer (OpenSSL) для криптографических операций.

Примечание: XCA является сторонним приложением, которое не поддерживается Cisco. Использование этого приложения предоставлено только для рисунка и простоты администрирования для администрирования S/MIME, тестирования и конфигурации. Для полного изложения и инструкций по XCA, обратитесь к [XCA - X Сертификатов и](#) документ [управления ключами](#).

Можно загрузить приложение XCA в любом из этих местоположений:

- Операционные системы Macintosh (OSX): [Sourceforge](#)

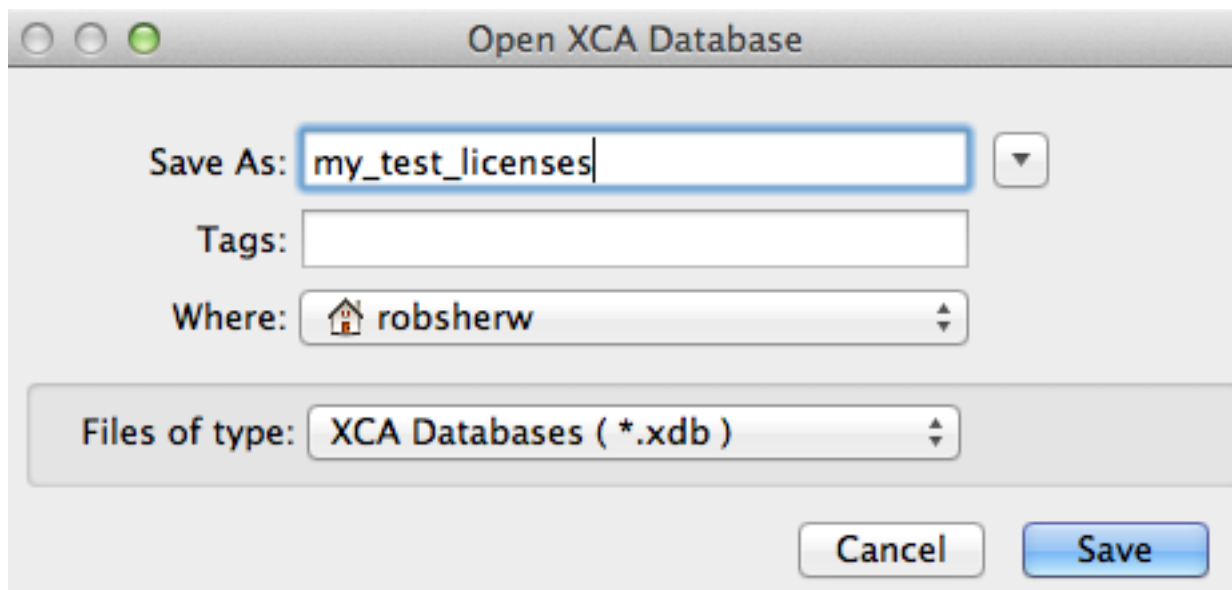
- Системы Microsoft Windows: [Softpedia](#)

Создайте сертификат

Выполните эти шаги для создания сертификата S/MIME:

1. Используйте приложение XCA, чтобы создать новую базу данных XCA или открыть текущую базу данных XCA, если вы уже существуете.

От строки меню перейдите к **Файлу> Новая База данных> <название DB по Вашему выбору>**:



Нажмите Save. Теперь необходимо ввести пароль для шифрования секретных ключей, которые привязаны к этой базе данных. Этот пароль только для базы данных XCA.




Нажмите **ОК** для завершения создания базы данных.

- От вкладки Certificates выберите **New Certificate**, и экран *Create x509 Certificate* появляется.

Никакие изменения не требуются от вкладки Source, поскольку могут использоваться значения по умолчанию:

The screenshot shows the 'Create x509 Certificate' dialog box. The 'Source' tab is selected. The 'Signing request' section has three checkboxes: 'Sign this Certificate signing request' (unchecked), 'Copy extensions from the request' (checked), and 'Modify subject of the request' (unchecked). The 'Signing' section has two radio buttons: 'Create a self signed certificate with the serial' (selected) and 'Use this Certificate for signing' (unchecked). The serial number field contains '1'. The 'Signature algorithm' dropdown is set to 'SHA 1'. The 'Template for the new certificate' dropdown is set to '[default] CA'. There are three buttons at the bottom: 'Apply extensions', 'Apply subject', and 'Apply all'.

От вкладки Subject введите необходимую информацию в раздел Составного имени. В разделе С закрытым ключом нажмите **Generate новый ключ** и выберите или **2048 битов** или **1024 бита** для размера ключа. Нажмите **Create**, чтобы генерировать Секретный ключ и привязать его к этому сертификату.

Create x509 Certificate 

Source Subject Extensions Key usage Netscape Advanced

Distinguished name

Internal name	royale298_1.calo.cisco.com	organizationName	Cisco
countryName	US	organizationalUnitName	TAC
stateOrProvinceName	North Carolina	commonName	royale298_1.calo.cisco.com
localityName	RTP	emailAddress	robsherw@cisco.com

Type	Content

Add
Delete

Private key

royale298_1.calo.cisco.com (RSA) Used keys too

От вкладки Extensions, в разделе Основных ограничений, выбирают **Certificate Authority** для Типа.

Примечание: Последующие Запросы подписи сертификата (CSR) могут быть подписаны через этот CA с набором Типа к **Не Определенный**.

В разделе Законности введите подробные данные согласно своим требованиям (365 дней по умолчанию). Можно принять решение добавить альтернативное имя субъекта (SAN) для Системы доменных имен (DNS), адреса электронной почты, и похожий с использованием кнопки **Edit** для той линии. От всплывающего окна SAN **нажмите Add** и выберите SAN тип и привязанное содержание. После того, как заверченный, нажмите **Apply**, чтобы применить эти изменения и возвратиться к окну вкладки Extensions:

Create x509 Certificate



Source Subject **Extensions** Key usage Netscape Advanced

Basic constraints

Type ▾

Path length Critical

Key identifier

Subject Key Identifier

Authority Key Identifier

Validity

Not before ▾

Not after ▾

Time range

▾

Midnight Local time No well-defined expiration

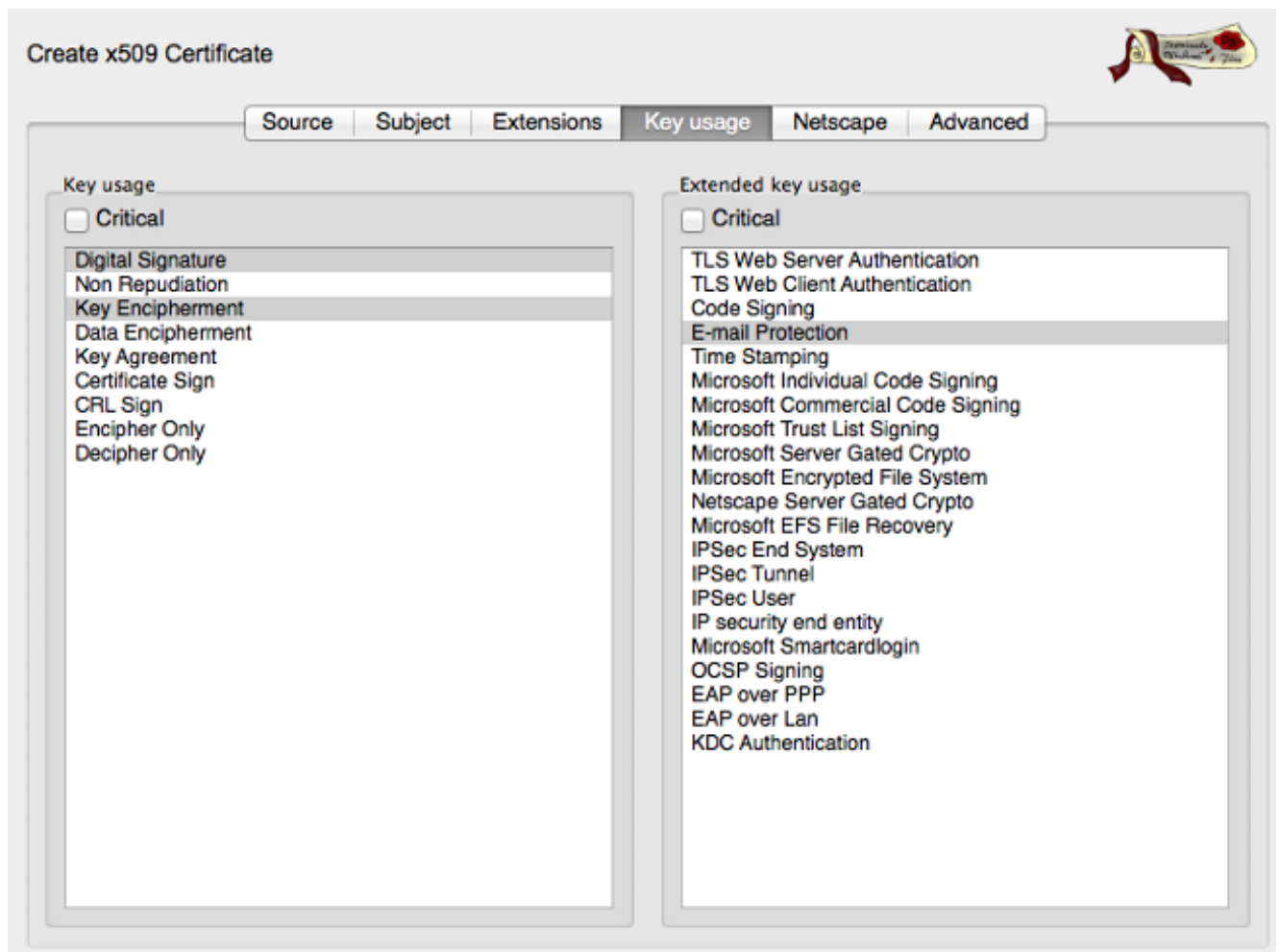
subject alternative name ✓

issuer alternative name

CRL distribution point

Authority Info Access ▾

От Ключевой вкладки использования, в Ключевом разделе использования, **Цифровой подписи** выделения и **Ключевой Шифровке**. В Расширенном ключевом разделе использования выделите **Почтовую Защиту**. Это требуемые элементы для S/MIME:

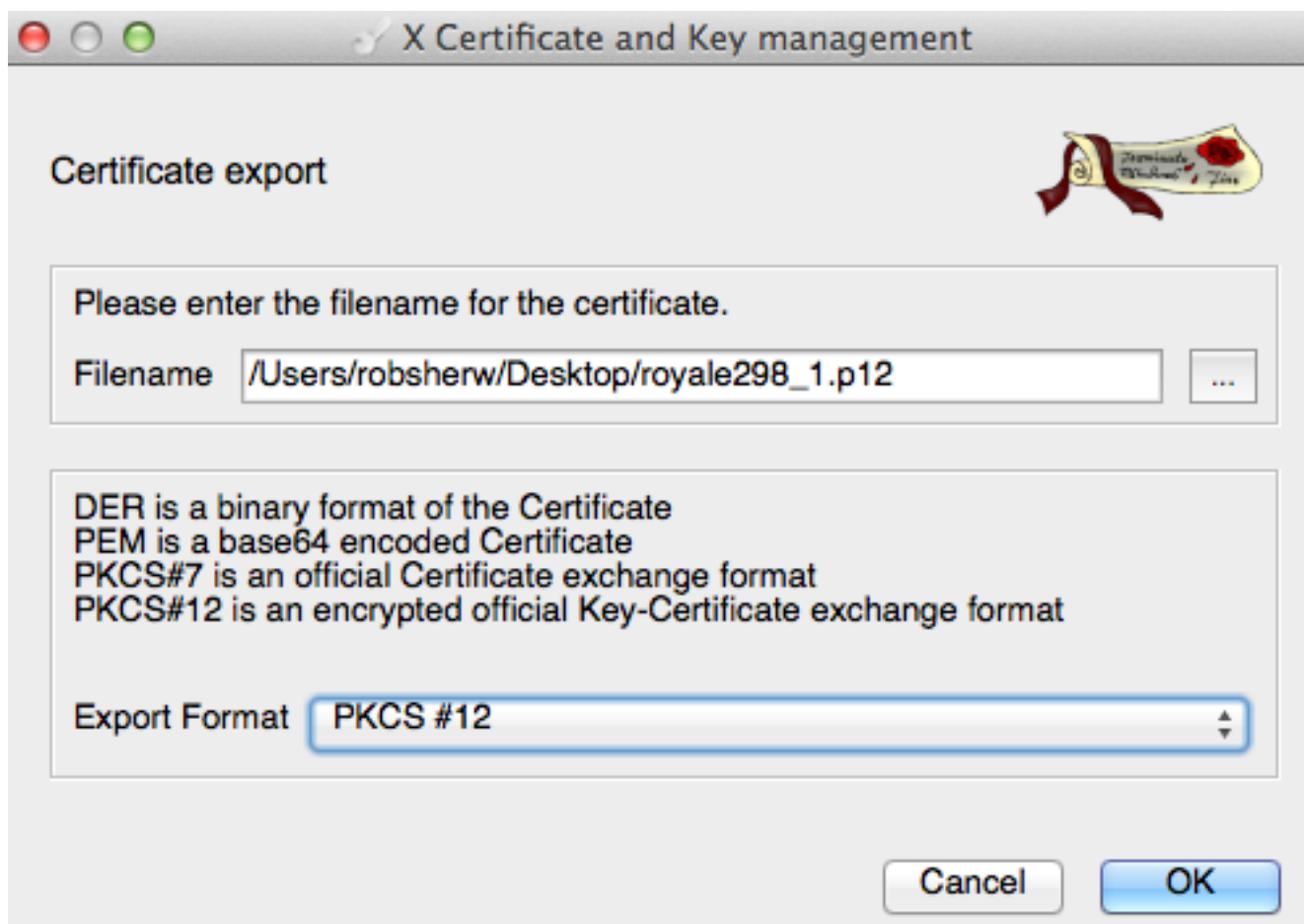


3. Нажмите **ОК** внизу экрана, и появляется всплывающее уведомление:

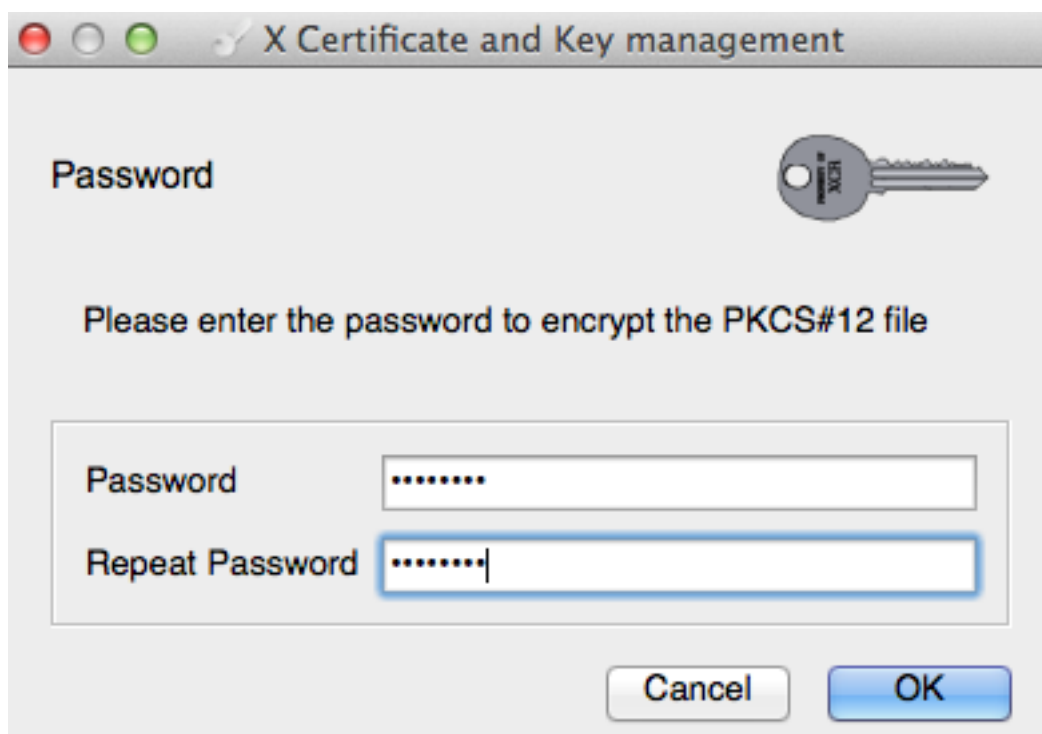


4. Ваш недавно созданный сертификат теперь появляется во вкладке Certificate. Нажмите сертификат, чтобы выделить его и нажать **Export**. Выберите имя файла, местоположение, к которому сертификат должен быть сохранен, и формат экспорта.

Примечание: Необходимо экспортировать сертификат и в PKCS12 и в отформатированных сертификатах Privacy Enhanced Mail (PEM). Сертификат PKCS12 сохраняет, поскольку .p12 отформатировал имя файла. Сертификат PEM сохраняет, поскольку .crt отформатировал имя файла.



Нажмите **OK**, и вам предоставляют пароль шифрования для сертификата PKCS12, который необходим, когда вы импортируете сертификат на ESA:



Примечание: Когда вы экспортируете отформатированный PEM сертификат, вам не предлагают для пароля, поскольку он не необходим.
Чтобы посмотреть детали сертификата, нажмите **Certificates** и переместитесь через

Статус, Предмет, Отправителя и вкладки Extensions:

Details of the certificate

Status Subject Issuer Extensions

Internal name royale298_1.calo.cisco.com

Signature Self signed Trusted

Key royale298_1.calo.cisco.com Serial 01

Signature algorithm sha1WithRSAEncryption

Fingerprints

MD5 88:BF:7F:E6:75:50:23:C8:09:3C:FB:C9:90:1C:7D:6F

SHA1 93:52:F3:FC:45:B5:89:C1:BF:29:26:2B:98:48:9E:B7:54:B5:E0:B1

Validity

November 24, 2014 10:41:00 AM EST November 24, 2015 10:41:00 AM EST Valid

На этом этапе ваш сертификат готов использоваться на вашем ESA.

Импортируйте сертификат

Теперь, когда сертификат создан, необходимо импортировать его на ESA. Выполните эти шаги для импорта сертификата:

1. Перейдите к **Сети>, Сертификаты> Добавляют Сертификат...> Сертификат импорта**.
2. Выберите PKCS12 (.p12) отформатированный файл, который вы создали в предыдущем разделе, введите пароль, который привязан к тому сертификату, и нажмите **Next**:

Add Certificate

Add Certificate

Add Certificate: Import Certificate

1 → Import Certificate: Choose File royale298_1.p12
PKCS#12 format is required.

2 → Enter Password: (required)

3 → Next

Cancel Next

3. Рассмотрите сертификат и нажмите **Submit** для фиксации изменений:

View Certificate royale298_1.calo.cisco.com

Add Certificate	
Certificate Name:	royale298_1.calo.cisco.com
Common Name:	royale298_1.calo.cisco.com
Organization:	Cisco
Organization Unit:	TAC
City (Locality):	RTP
State (Province):	North Carolina
Country:	US
Signature Issued By:	Common Name (CN): royale298_1.calo.cisco.com Organization (O): Cisco Organizational Unit (OU): TAC Issued On: Nov 24 15:41:00 2014 GMT Expires On: Nov 24 15:41:00 2015 GMT <small>If you would like a globally recognized signed certificate: 1. Download Certificate Signing Request, 2. Submit this to a certificate authority, 3. Once you receive the signed certificate, upload it below.</small>
	Download Certificate Signing Request...
Upload Signed Certificate:	<input type="button" value="Choose File"/> No file chosen <small>Uploading a new certificate will overwrite the existing certificate.</small>
Intermediate Certificates (optional):	<small>Upload intermediate certificates if applicable.</small>

На этом этапе ваш сертификат теперь готов использоваться для S/MIME на вашем ESA.

Привяжите сертификат PEM

Необходимо теперь добавить отформатированный PEM сертификат к Открытым ключам S/MIME. Выполните эти шаги для добавления отформатированного PEM сертификата:

1. Перейдите для **Отправки по почте Политики>, Открытые ключи S/MIME> Добавляют Открытый ключ....**
2. Введите имя, как требуется.
3. Откройте PEM (.crt) отформатированный сертификат в соответствующем текстовом редакторе (таком как Блокнот ++ или Atom).
4. Скопируйте содержание с **-----СЕРТИФИКАТА BEGIN-----** через **-----КОНЕЧНЫЙ СЕРТИФИКАТ-----**.
5. Вставьте это содержание в раздел С открытым ключом S/MIME и нажмите **Submit**:

Add S/MIME Public Key

Add Public Key	
Name:	royale298_1_public_key
S/MIME Public Key:	<pre>-----BEGIN CERTIFICATE----- MIIEAJCCAuqAAwIBAgIBATANBqkqkhiG9w0BAQUFADCBmIEMAKGA1UERhMCVVMx FzAVBqNVBAgTDk5xcnRoIENhcm9saW5hMQwwCgYDVQQHEwNSVFAxDjAMBgNVBAoT BUlNpc2NvMQwwCgYDVQQLEwNUQUUMxIzAhBgNVBAMMGnJveWFsZTI1OF8xLmNhbG8u Y2lyY29uY29tMSEwHwYJKoZIhvcNAQkBFhJyb2JzeGVyd0BjaXNjby5jb20wHhcN MTQxMTI0MTU0MTAwWbcNMTUxMTU0MTU0MTAwWjCBmIEMAKGA1UERhMCVVMx BgNVBAgTDk5xcnRoIENhcm9saW5hMQwwCgYDVQQHEwNSVFAxDjAMBgNVBAoTBUlN c2NvMQwwCgYDVQQLEwNUQUUMxIzAhBgNVBAMMGnJveWFsZTI1OF8xLmNhbG8uY2ly Y29uY29tMSEwHwYJKoZIhvcNAQkBFhJyb2JzeGVyd0BjaXNjby5jb20wggEiMA0G CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQAQEMocaf8ezvRTICmBYMIQ12aEWTd ISA+LxwEgkDdmY+jMiRm1+njBDDF1V9nw8PhDQx7UhhK8r0m2aNCwDjaLY16Mhd4 JJHThNe/BCwxFXZVaCk9Vfxt5Dp18ExtAfcZlvrXgkJ2YUkDZKE6huo4ZaY0Ib xTghWwMAF3oAsXRR+MTwQXJ8fvaIy6Gee5QioRtRwY+2+HKATWjYuuo9Blef2E 4MlbfenRlIRkm5cUJ2ZrtUjWe7JHuZCgDIvDJEdoMUcUsqZA5xG6a55yAfp4mG QCI9zmUc02nCcIaDd1cWthr5x7zpwj7wlevrdej2dfvLJNrcGne/CDfKNAgMBAAGj -----</pre>

6. Передайте все изменения. На этом этапе ваш Открытый ключ S/MIME теперь установлен для вашего ESA.

Дополнительные сведения

- [AsyncOS 9.0 для почтового руководства пользователя](#)
- [Cisco Systems – техническая поддержка и документация](#)