

Возобновите сертификат на устройстве безопасности электронной почты

Содержание

[Введение](#)

[Возобновите сертификат на ESA](#)

[Обновите сертификат через GUI](#)

[Обновите сертификат через CLI](#)

[Дополнительные сведения](#)

Введение

Этот документ описывает, как возобновить просроченный сертификат на Cisco Email Security Appliance (ESA).

Возобновите сертификат на ESA

Если у вас есть просроченный сертификат на вашем ESA (или тот, который скоро истечет), можно просто обновить текущий сертификат:

1. Загрузите файл Запроса подписи сертификата (CSR).
2. Предоставьте файл CSR своему Центру сертификации (CA) и запросите Privacy Enhanced Mail (PEM) (X.509) подписанный сертификат.
3. Обновите свой текущий сертификат с помощью одного из методов, которые описаны в разделах, которые придерживаются.

Обновите сертификат через GUI

Для начала перейдите к **Сети > Сертификаты** от GUI устройства. Откройте свой сертификат и загрузите файл CSR через ссылку, которую показывают в следующем образе. Если ESA является участником кластера, необходимо проверить другие сертификаты члена кластера и использовать тот же метод для каждой машины. С этим методом секретный ключ остается на ESA. Последнему шагу должен был подписать сертификат ваш CA.

Например:

(Province):	NC
Country:	US
Issued By:	<p>Common Name (CN): tarheel.rtp Organization (O): Cisco Systems Inc Organizational Unit (OU): RTP TAC Issued On: Jul 25 02:27:49 2013 GMT Expires On: Jul 25 02:27:49 2015 GMT</p> <p><i>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.</i></p> <p>Upload Signed Certificate: <input type="button" value="Browse..."/> No file selected. <i>Uploading a new certificate will overwrite the existing certificate.</i></p> <p>Download Certificate Signing Request...</p>
(optional):	<i>Upload intermediate certificates if applicable.</i>

1. Файл CSR загрузки к вашему локальному компьютеру, как показано в предыдущем образе.
2. Предоставьте файл CSR своему CA и запросите, чтобы X.509 отформатировал сертификат.
3. Как только вы получаете файл PEM, импортируете сертификат через раздел *Подписанного сертификата Загрузки*. Кроме того, загрузите промежуточный сертификат (при наличии) в *дополнительном* разделе.
4. Отправьте и передайте изменения.
5. Возвратитесь к основной странице Certificates (**Сеть**> **Сертификаты** от GUI).
6. Проверьте, что новая дата окончания действия появляется и что сертификат показывает как **ДОПУСТИМЫЙ/АКТИВНЫЙ**.
7. Отправьте и передайте изменения.

Обновите сертификат через CLI

Можно также обновить сертификат через CLI. Этот метод мог бы казаться более интуитивным, как приглашения находятся в формате вопроса/ответа.

Например:

```
myexample.com> certconfig
```

Choose the operation you want to perform:

- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
 - CERTAUTHORITY - Manage System and Customized Authorities
 - CRL - Manage Certificate Revocation Lists
- ```
[]> certificate
```

List of Certificates

| Name      | Common Name          | Issued By            | Status | Remaining |
|-----------|----------------------|----------------------|--------|-----------|
| tarheel.r | myexample.com        | myexample.com        | Active | 327 days  |
| test      | test                 | test                 | Valid  | 3248 days |
| Demo      | Cisco Appliance Demo | Cisco Appliance Demo | Active | 1570 days |

Choose the operation you want to perform:

- IMPORT - Import a certificate from a local PKCS#12 file
  - PASTE - Paste a certificate into the CLI
  - NEW - Create a self-signed certificate and CSR
  - EDIT - Update certificate or view the signing request
  - EXPORT - Export a certificate
  - DELETE - Remove a certificate
  - PRINT - View certificates assigned to services
- [> edit

1. [myexample.com] C=US,CN=myexample.com,L=RTP,O=Cisco Inc.,ST=NC,OU=TAC
2. [test] C=US,CN=test,L=yanceyville,O=test,ST=NC,OU=another test

Select the certificate profile you wish to edit:

[> 1

Would you like to update the existing public certificate? [N]> y

Paste public certificate in PEM format (end with '.')

```
-----BEGIN CERTIFICATE-----
FR3XlVd6h3cMPWNghAeWGYlcMKMr5n2M3L9
DdeLZOOD0ekCqTxG7OD8tFfJzgvhEQwVDj0zRjUk9yjmoeLx8GNgm4gB6v2QPm+f
ajNHbf9lKRUFy9AHyMRsa+DmpWcvzvFiyP28vSxAUIT3WMGJwwMxRcXOB/jF5V66
8caFN0A7tDyUt/6YCWlKFeuCHaOGBRgFFp71Frsh5uZq1C70wE07cZP5Mm3AWjds
3ZDvi/oJBn5nCR8HuvkDVNO6z9NVIE06gP564n6RagMBAAEwDQYJKoZIhvcNAQEF
BQADggEBAA/BTYiw+0wAh1q3z1yfW6oVyx03/bGEdeT0TE8U3naBBKM/Niu8zAwK
7yS4tkWK3b96HK98IKWuxOVSY0EivW8EUWSalK/2zsLEp5/iuZ/eAfdshRjDQKn3
H541MuowGaQc6NGtLjIfFet5pQ7w7R44z+4oSXYsT9FLH78/w5DdLf6Rk696c1p
hb9U9lg7SnKvDrwLZ6i4Sn0TA6bl/z0p9DuvVSwtNEHcn3kCbmbFpsD2Hd6EWKD
70zXapUp6/xG79pc2gFXHfg0RcmsozcmHPCjXjnL40jpUExonSjffB3HhSKDqjhf
A0uN6Psgar9yz8M/B3ego34Nq3al/F4=
-----END CERTIFICATE-----
.
```

C=US,CN=myexample.com,L=RTP,O=Cisco Inc.,ST=NC,OU=TAC

Do you want to add an intermediate certificate? [N]> Y

Paste intermediate certificate in PEM format (end with '.')

[Removed for simplicity]

Do you want to add another intermediate certificate? [N]>

Would you like to remove an intermediate certificate? [N]>

Do you want to view the CSR? [Y]>

```
-----BEGIN CERTIFICATE REQUEST-----
MIICPjCCAY4CAQAwYTELMAkGA1UEBhMCVVMxZDASBgNVBAMTC3RhcmlhZGZwucnRw
MQwwCgYDVQQHEWNSVFAXEzARBgNVBAoTCkNpc2NvIEluYy4xCzAJBgNVBAGTAk5D
MQwwCgYDVQQLEwNUQUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5
gnqxG/GgDsxfOB7iWpNkCZpedKC5Qj5UpOEuMMx/OsAUXUNblJNktGMmW7dq6p9Z
4zAofRMgQFR3XlVd6h3cMPWNghAeWGYlcMKMr5n2M3L9DdeLZOOD0ekCqTxG7OD8
tFfJzgvhEQwVDj0zRjUk9yjmoeLx8GNgm4gB6v2QPm+fa jNHbf9lKRUFy9AHyMRs
a+DmpWcvzvFiyP28vSxAUIT3WMGJwwMxRcXOB/jF5V668caFN0A7tDyUt/6YCWlK
FeuCHaOGBRgFFp71Frsh5uZq1C70wE07cZP5Mm3AWjds3ZDvi/oJBn5nCR8HuvkD
VNO6z9NVIE06gP564n6RagMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEAOpN8fD+H
Wa7n+XTwAb1jyC7yrjp9Ll08bc6Viy4bolrS15DxqAkvtCqssK+xhAScX2j9hxq2
```

```
pHBp8D5wMEMSUR39Jw77HRWNKHltUauIJUc3wEOeZ3b6pOUJA1NQenMBZJby7Hgw
0wV9X42JmDfwnBpWUW+rEyZHm0N9AATdgxmpFGvKieiOM+fA0BKNxc7p0MMdcaBw
cQr/+bSfF3dWR8q8FAwS51RJ2cMQGpTZ2sLD54GbudpJqYUvjky1sYcn2USqupFn
WbhZArh0AQiSxolI+B6pgk/GE+50fNAB01IVqAYzzG41V76p17soBp6mXr7dxOGL
YM21mN12Rq3BkQ==
```

-----END CERTIFICATE REQUEST-----

List of Certificates

| Name      | Common Name          | Issued By            | Status | Remaining |
|-----------|----------------------|----------------------|--------|-----------|
| tarheel.r | myexample.com        | myexample.com        | Active | 327 days  |
| test      | test                 | test                 | Valid  | 3248 days |
| Demo      | Cisco Appliance Demo | Cisco Appliance Demo | Active | 1570 days |

Choose the operation you want to perform:

- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- EDIT - Update certificate or view the signing request
- EXPORT - Export a certificate
- DELETE - Remove a certificate
- PRINT - View certificates assigned to services

[ ]>

Choose the operation you want to perform:

- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists

[ ]>

>commit

## Дополнительные сведения

- [Требования установки сертификатов ESA](#)
- [Установите сертификат SSL через CLI на ESA](#)
- [Гарантируйте, что может быть проверен ваш сертификат ESA](#)
- [Добавьте/Импортируйте Новый Сертификат PKCS#12 на GUI ESA Cisco](#)
- [Cisco Systems – техническая поддержка и документация](#)