

Renove um certificado em uma ferramenta de segurança do email

Índice

[Introdução](#)

[Renove um certificado no ESA](#)

[Atualize o certificado através do GUI](#)

[Atualize o certificado através do CLI](#)

[Informações Relacionadas](#)

Introdução

Este original descreve como renovar um certificado expirado na ferramenta de segurança do email de Cisco (ESA).

Renove um certificado no ESA

Se você tem um certificado expirado em seu ESA (ou em um que expirará logo), você pode simplesmente atualizar o certificado atual:

1. Transfira o arquivo da solicitação de assinatura de certificado (CSR).
2. Forneça o arquivo CSR a seu Certificate Authority (CA) e peça um Privacy Enhanced Mail (PEM) (X.509) certificado assinado.
3. Atualize seu certificado atual através de um dos métodos que são descritos nas seções que seguem.

Atualize o certificado através do GUI

Note: Estas etapas supõem que o certificado esteve criado, submetido, e comprometido à configuração ESA. Se você cria um certificado novo, recorde submeter-se e comprometer para salvar o certificado ao dispositivo antes que você transfira o CSR.

A fim começar, navegue à **rede > aos Certificados do** dispositivo GUI. Abra seu certificado e transfira o arquivo CSR através do link que é mostrado na imagem seguinte. Se o ESA é um membro de um conjunto, você deve verificar os outros Certificados do membro de grânulos e usar o mesmo método para cada máquina. Com este método, a chave privada permanece no ESA. A última etapa é ter o certificado assinado por seu CA.

Aqui está um exemplo:

(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>
(optional):	Upload intermediate certificates if applicable.

1. Arquivo da transferência CSR a seu computador local, segundo as indicações da imagem anterior.
2. Forneça o arquivo CSR a seu CA e peça um certificado formatado **X.509**.
3. Uma vez que você recebe o arquivo PEM, importe o certificado através da seção do *certificado assinado da transferência de arquivo pela rede*. Também, transfira arquivos pela rede o certificado intermediário (se disponível) na seção *opcional*.
4. Submeta e comprometa as mudanças.
5. Retorne à página principal dos Certificados (**rede > Certificados do GUI**).
6. Verifique que a data de expiração nova aparece e que o certificado mostra como **VALID/ACTIVE**.
7. Submeta e comprometa as mudanças.

Atualize o certificado através do CLI

Você pode igualmente atualizar o certificado através do CLI. Este método pôde parecer mais intuitivo, como as alertas estão no formato da pergunta/resposta.

Aqui está um exemplo:

```
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+4oSWXYsT9FLH78/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
MQwwCgYDVQQHEWNSVFAxZzARBgNVBAoTCkNpc2NvIEluYy4xZCZAJBgNVBAGTAk5D
MQwwCgYDVQQLEWNUQUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQc5
gnqxG/GgDsxfOB7iWpNkCZpedKC5Qj5UpOEuMMx/OsAUXUNblJNktGMmW7dq6p9Z
4zAofRMgQFR3XlVd6h3cMPWNghAeWGYlcMKMr5n2M3L9DdeLZOOD0ekCqTxG7OD8
tFfJzgvhEQwVDj0zRjUk9yjmoeLx8GNgm4gB6v2QPm+fa jNHbf9lKRUFy9AHyMRs
a+DmpWcvzvFiyP28vSxAUIT3WMGJwwMxRcXOB/jF5V668caFN0A7tDyUt/6YCWlK
FeuCHaOGBRgFFp71Frsh5uZq1C70wE07cZP5Mm3AWjds3ZDvi/oJBn5nCR8HuvkD
VNO6z9NVIE06gP564n6RagMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEAOpN8fD+H
Wa7n+XTwAb1jyC7yrjp9Llo8bc6Viy4bolrS15DxqAkvtCqssK+xhAScX2j9hxq2
```

```
pHBp8D5wMEMSUR39Jw77HRWNKHltUauIJUc3wEOeZ3b6pOUJA1NQenMBZJby7Hgw
0wV9X42JmDfwNBpWUW+rEyZHm0N9AATdgxmpFGvKieiOM+fA0BKNxc7p0MMdcaBw
cQr/+bSfF3dwr8q8FAwS51RJ2cMQGpTZ2sLD54GbudpJqYUvjky1sYcn2USqupFn
WbhZArh0AQiSxolI+B6pgk/GE+50fNAB0lIVqAYzzG41V76p17soBp6mXr7dxOGL
YM2lmN12Rq3BkQ==
```

-----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

Informações Relacionadas

- [Exigências da instalação certificada ESA](#)
- [Instale um certificado SSL através do CLI em um ESA](#)
- [Assegure-se de que seu certificado ESA possa ser verificado](#)
- [Certificado novo do PKCS-12 adicionar/importação em Cisco ESA GUI](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)