Renueve un certificado en un dispositivo de seguridad del correo electrónico

Contenido

Introducción

Este documento describe cómo renovar un certificado vencido en el dispositivo de seguridad del correo electrónico de Cisco (ESA).

Renueve un certificado en el ESA

Si usted tiene un certificado vencido en su ESA (o uno que pronto expire), usted puede poner al día simplemente el certificado actual:

1. Descargue el archivo del pedido de firma de certificado (CSR).

2. Proporcione el archivo CSR a su Certificate Authority (CA) y pida un certificado firmado de Privacy Enhanced Mail (PEM) (X.509).

3. Ponga al día su certificado actual vía uno de los métodos que se describen en las secciones que siguen.

Ponga al día el certificado vía el GUI

Para comenzar, navegue a la **red > a los Certificados del** dispositivo GUI. Abra su certificado y descargue el archivo CSR vía el link que se muestra en la imagen siguiente. Si el ESA es un miembro de un cluster, usted debe verificar los otros Certificados del miembro de clúster y utilizar el mismo método para cada máquina. Con este método, sigue habiendo la clave privada en el ESA. El paso más reciente es hacer el certificado firmar por su CA.

Aquí tiene un ejemplo:

1. Archivo de la descarga CSR a su computadora local, tal y como se muestra en de la imagen anterior.

2. Proporcione el archivo CSR a su CA y pida un certificado formatado **X.509**.

3. Una vez que usted recibe el archivo PEM, importe el certificado vía la sección del *certificado firmado de la carga*. También, cargue el certificado intermedio (si está disponible) en la sección *opcional*.

4. Someta y confíe los cambios.

5. Vuelva a la página principal de los Certificados (**red > Certificados del** GUI).

6. Verifique que aparezca la nueva fecha de vencimiento y que el certificado muestra como **VALID/ACTIVE**.

7. Someta y confíe los cambios.

Ponga al día el certificado vía el CLI

Usted puede también poner al día el certificado vía el CLI. Este método pudo parecer más intuitivo, como los prompts están en el formato de la pregunta/de la respuesta.

Aquí tiene un ejemplo:

```
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/6YCW1KFeuCHaOGBRgFFp71Frsh5uZq1C70wE07cZP5Mm3AWjds
3ZDvi/oJBn5nCR8HuvkDVNO6z9NVIE06gP564n6RAgMBAAEwDQYJKoZIhvcNAQEF
BQADggEBAA/BTYiw+0wAh1q3z1yfW6oVyx03/bGEdeT0TE8U3naBBKM/Niu8zAwK
7yS4tkWK3b96HK98IKWuxOVSY0EivW8EUWSalK/2zsLEp5/iuZ/eAfdsHrJdQKn3
H541MuowGaQc6NGtLjIfFet5pQ7w7R44z+4oSWXYsT9FLH78/w5DdLf6Rk696c1p
hb9U9lg7SnKvDrwLZ6i4Sn0TA6bl/z0p9DuvVSwWTNEHcn3kCbmbFpsD2Hd6EWKD
70zXapUp6/xG79pc2gFXHfg0RcmsozcmHPCjXjnL4OjpUExonSjffB3HhSKDqjhf
A0uN6Psgar9yz8M/B3ego34Nq3a1/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-----
MIICpjCCAY4CAQAwYTELMAkGA1UEBhMCVVMxFDASBgNVBAMTC3RhcmhlZWwucnRw
MQwwCgYDVQQHEwNSVFAxEzARBgNVBAoTCkNpc2NvIEluYy4xCzAJBgNVBAgTAk5D
MQwwCgYDVQQLEwNUQUMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5
gnqxG/GgDsxfOB7iWpNkCZpedKC5Qj5UpOEuMMx/OsAUXUNblJNktGMmW7dq6p9Z
4zAofRMgQFR3XlVd6h3cMPWNgHAeWGYlcMKMr5n2M3L9DdeLZOOD0ekCqTxG7OD8
tFfJzgvhEQwVDj0zRjUk9yjmoeLx8GNgm4gB6v2QPm+fajNHbf9lKRUFy9AHyMRs
a+DmpWcvzvFiyP28vSxAUIT3WMGJwwMxRcXOB/jF5V668caFN0A7tDyUt/6YCW1K
FeuCHaOGBRgFFp71Frsh5uZq1C70wE07cZP5Mm3AWjds3ZDvi/oJBn5nCR8HuvkD
VNO6z9NVIE06gP564n6RAgMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEAOpN8fD+H
Wa7n+XTwAb1jyC7yrjp9Llo8bc6Viy4bolrS15DxqAkvTCqssK+xhAScX2j9hxq2
```

```
pHBp8D5wMEmSUR39Jw77HRWNKHltUauIJUc3wEOeZ3b6pOUJAlNQenMBZJby7Hgw
0wV9X42JmDfwNBpWUW+rEyZHm0N9AATdgxmpFGvKIeiOM+fA0BKNxc7p0MMdcaBw
cQr/+bSfF3dwR8q8FAwS51RJ2cMQGpTZ2sLD54GbudpJqYUvjky1sYcn2USqupFn
WbhzArh0AQiSxolI+B6pgk/GE+50fNABOlIVqAYzzG41V76p17soBp6mXr7dxOGL
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
```

Información Relacionada

- Requisitos de la instalación del certificado ESA
- Instale un certificado SSL vía el CLI en un ESA
- Asegúrese de que su certificado ESA pueda ser verificado
- Nuevo certificado del PKCS-12 agregue/de la importación en Cisco ESA GUI
- Soporte Técnico y Documentación - Cisco Systems