Reinicializar un certificado en un dispositivo de seguridad de correo electrónico

Contenido

Introducción

Este documento describe cómo renovar un certificado caducado en el dispositivo de seguridad Cisco Email Security Appliance (ESA).

Renovación de un certificado en el ESA

Si tiene un certificado caducado en su ESA (o uno que caduca pronto), simplemente puede actualizar el certificado actual:

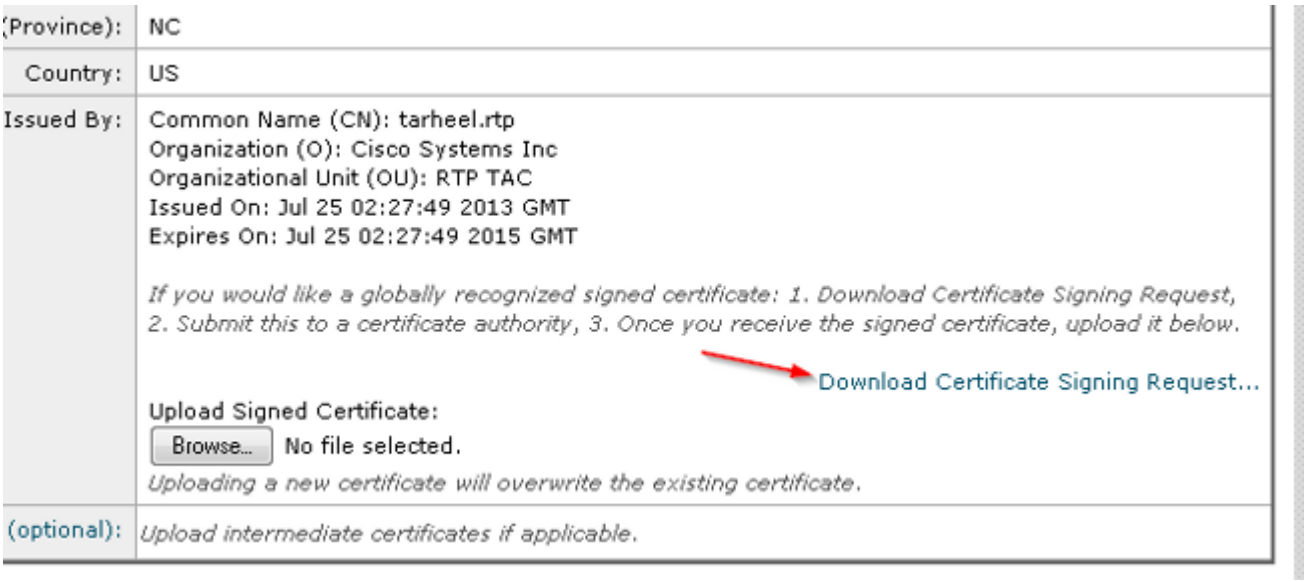
1. Descargue el archivo de solicitud de firma de certificado (CSR).
2. Proporcione el archivo CSR a su autoridad de certificación (CA) y solicite un certificado firmado por Privacy-Enhanced Mail (PEM) (X.509).
3. Actualice el certificado actual mediante uno de los métodos descritos en las secciones mencionadas.

Actualizar el certificado mediante la GUI

> **Nota**: En estos pasos se supone que el certificado se ha creado, enviado y confirmado en la configuración de ESA. Si crea un nuevo certificado, no olvide enviar y guardar el certificado en el dispositivo antes de descargar el CSR.

Para comenzar, vaya a Network > Certificates desde la GUI del dispositivo. Abra el certificado y descargue el archivo CSR a través del enlace que se muestra en la siguiente imagen. Si el ESA es miembro de un clúster, debe comprobar los otros certificados de miembro del clúster y utilizar el mismo método para cada equipo. Con este método, la clave privada permanece en el ESA. El último paso es que la CA firme el certificado.

Aquí tiene un ejemplo:



1. Descargue el archivo CSR en el equipo local, como se muestra en la imagen anterior.
2. Proporcione el archivo CSR a su CA y solicite una X.509 certificado con formato.
3. Una vez que reciba el archivo PEM, importe el certificado a través de la sección "Cargar certificado firmado". Cargue también el certificado intermedio (si está disponible) en la sección opcional.
4. Envíe y confirme los cambios.
5. Volver a la página principal de certificados (Network > Certificates desde la interfaz gráfica de usuario).
6. Verifique que aparezca la nueva fecha de vencimiento y que el certificado se muestre como **VÁLIDO/ACTIVO**.
7. Envíe y confirme los cambios.

Actualizar el certificado mediante la CLI

También puede actualizar el certificado mediante la CLI. Este método parece más intuitivo, ya que las indicaciones están en formato de pregunta/respuesta.

Aquí tiene un ejemplo:

```
<#root>

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 instalación del certificado ESA
- Instalar un certificado SSL a través de la CLI en un ESA
- Agregar/importar nuevo certificado PKCS#12 en la GUI de Cisco ESA
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).