Reinizializzare un certificato in Email Security Appliance

Sommario

Introduzione

Questo documento descrive come rinnovare un certificato scaduto su Cisco Email Security Appliance (ESA).

Rinnovo di un certificato sull'ESA

Se il certificato dell'ESA è scaduto (o sta per scadere), è sufficiente aggiornare il certificato corrente:

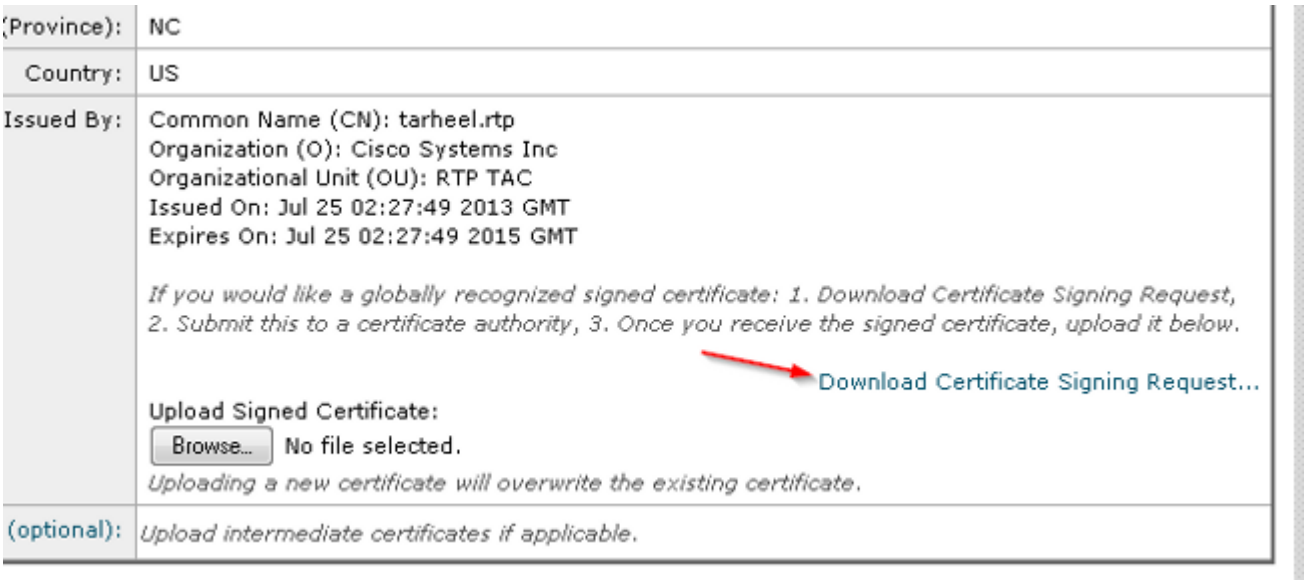
1. Scaricare il file CSR (Certificate Signing Request).
2. Fornire il file CSR all'autorità di certificazione (CA) e richiedere un certificato firmato PEM (Privacy-Enhanced Mail) (X.509).
3. Aggiornare il certificato corrente utilizzando uno dei metodi descritti nelle sezioni indicate.

Aggiornare il certificato tramite la GUI

> **Nota**: questa procedura presuppone che il certificato sia stato creato, sottomesso e vincolato alla configurazione ESA. Se si crea un nuovo certificato, ricordarsi di inviare e salvare il certificato all'accessorio prima di scaricare il CSR.

Per iniziare, passare a Network > Certificates dalla GUI dell'accessorio. Aprire il certificato e scaricare il file CSR tramite il collegamento visualizzato nell'immagine seguente. Se l'ESA è un membro di un cluster, è necessario verificare gli altri certificati di membro del cluster e utilizzare lo stesso metodo per ogni computer. Con questo metodo, la chiave privata rimane sull'ESA. L'ultimo passaggio consiste nel far firmare il certificato dalla CA.

Di seguito è riportato un esempio:



1. Scaricare il file CSR sul computer locale, come illustrato nell'immagine precedente.
2. Fornire il file CSR alla CA e richiedere un X.509 certificato formattato.
3. Dopo aver ricevuto il file PEM, importare il certificato tramite la sezione 'Carica certificato firmato'. Inoltre, caricare il certificato intermedio (se disponibile) nella sezione facoltativa.
4. Inviare e confermare le modifiche.
5. Torna alla pagina principale Certificati (Network > Certificates dalla GUI).
6. Verificare che venga visualizzata la nuova data di scadenza e che il certificato sia **VALIDO/ATTIVO**.
7. Inviare e confermare le modifiche.

Aggiornare il certificato dalla CLI

è possibile anche aggiornare il certificato dalla CLI. Questo metodo sembra più intuitivo, in quanto i prompt sono in formato domanda/risposta.

Di seguito è riportato un esempio:

```
<#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

Informazioni correlate

- Requisiti per l'installazione del certificato ESA
- Installare un certificato SSL tramite la CLI su un'ESA
- Aggiunta/importazione di un nuovo certificato PKCS#12 sull'interfaccia utente di Cisco ESA
- Documentazione e supporto tecnico â€“ Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).