

# Erneute Initialisierung eines Zertifikats auf einer E-Mail-Security-Appliance

## Inhalt

[Einleitung](#)

[Erneuerung eines Zertifikats auf der ESA](#)

[Aktualisieren des Zertifikats über die Benutzeroberfläche](#)

[Aktualisieren des Zertifikats über die CLI](#)

[Zugehörige Informationen](#)

## Einleitung

In diesem Dokument wird die Verlängerung eines abgelaufenen Zertifikats der Cisco E-Mail Security Appliance (ESA) beschrieben.

## Erneuerung eines Zertifikats auf der ESA

Wenn Ihr ESA-Zertifikat abgelaufen ist (oder bald abläuft), können Sie das aktuelle Zertifikat einfach aktualisieren:

1. CSR-Datei (Certificate Signing Request) herunterladen
2. Übergeben Sie die CSR-Datei an Ihre Zertifizierungsstelle (Certificate Authority, CA), und fordern Sie ein mit Privacy-Enhanced Mail (PEM) (X.509) signiertes Zertifikat an.
3. Aktualisieren Sie Ihr aktuelles Zertifikat mithilfe einer der Methoden, die in den genannten Abschnitten beschrieben werden.

## Aktualisieren des Zertifikats über die Benutzeroberfläche

---

**Hinweis:** Bei diesen Schritten wird davon ausgegangen, dass das Zertifikat erstellt, übermittelt und in die ESA-Konfiguration übernommen wurde. Wenn Sie ein neues Zertifikat erstellen, denken Sie daran, das Zertifikat einzureichen und auf der Appliance zu speichern, bevor Sie die CSR-Datei herunterladen.

---

Navigieren Sie zunächst zu `Network > Certificates` über die Appliance-GUI. Öffnen Sie Ihr Zertifikat, und laden Sie die CSR-Datei über den Link herunter, der im nächsten Bild angezeigt wird. Wenn die ESA zu einem Cluster gehört, müssen Sie die anderen Cluster-Member-Zertifikate überprüfen und für jeden Computer dieselbe Methode verwenden. Bei dieser Methode verbleibt der private Schlüssel auf der ESA. Als letzter Schritt muss das Zertifikat von Ihrer Zertifizierungsstelle signiert werden.

Hier ein Beispiel:

(Province):	NC
Country:	US
Issued By:	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  <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>  <a href="#">Download Certificate Signing Request...</a>  Upload Signed Certificate: <input type="button" value="Browse..."/> No file selected. <i>Uploading a new certificate will overwrite the existing certificate.</i>
(optional):	Upload intermediate certificates if applicable.

1. Laden Sie die CSR-Datei auf Ihren lokalen Computer herunter, wie im vorherigen Bild gezeigt.
2. Geben Sie die CSR-Datei an Ihre Zertifizierungsstelle weiter, und fordern Sie eine x.509 formatiertes Zertifikat.
3. Sobald Sie die PEM-Datei erhalten haben, importieren Sie das Zertifikat über den Abschnitt "Signiertes Zertifikat hochladen". Laden Sie auch das Zwischenzertifikat (falls verfügbar) in den optionalen Abschnitt hoch.
4. Senden und bestätigen Sie die Änderungen.
5. Zurück zur Hauptseite Zertifikate (Network > Certificates über die GUI).
6. Überprüfen Sie, ob das neue Ablaufdatum angezeigt wird und das Zertifikat als **GÜLTIG/AKTIV** angezeigt wird.
7. Senden und bestätigen Sie die Änderungen.

## Aktualisieren des Zertifikats über die CLI

Sie können das Zertifikat auch über die CLI aktualisieren. Diese Methode erscheint intuitiver, da die Eingabeaufforderungen im Frage-Antwort-Format vorliegen.

Hier ein Beispiel:

```
<#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

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-----

```
FR3X1Vd6h3cMPWNghAeWGY1cMKMr5n2M3L9
DdeLZ00D0ekCqTxG70D8tFfJzgvhEQwVDj0zRjUk9yjmoeLx8GNgm4gB6v2QPm+f
ajNHbf91KRUFy9AHyMRsa+DmpWcvzvFiyP28vSxAUIT3WMGJwwMxRcXOB/jF5V66
8caFN0A7tDyUt/6YCW1KFeuCHaOGBRgFFp71Frsh5uZq1C70wE07cZP5Mm3AWjds
3ZDvi/oJBn5nCR8HuvkDVN06z9NVIE06gP564n6RAGMBAAEwDQYJKoZIhvcNAQEF
BQADggEBAA/BTYiw+0wAh1q3z1yfW6oVyx03/bGEdeT0TE8U3naBBKM/Niu8zAwK
7yS4tkWK3b96HK98IKWux0VSY0EivW8EUWSa1K/2zsLEp5/iuZ/eAfdshRjDQKn3
H541MuowGaQc6NGtLjIfFet5pQ7w7R44z+4oSWXYsT9FLH78/w5DdLf6Rk696c1p
hb9U9lg7SnKvDrwLZ6i4Sn0TA6b1/z0p9DuvVSwwTNEHcn3kCbmbFpsD2Hd6EWKD
70zXapUp6/xG79pc2gFXHfg0RcmsozcmHPCjXjnL40jpUExonSjffB3HhSKDqjhf
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-----

```
MIICPjCCAY4CAQAwYTELMAkGA1UEBhMCVVMxZDASBgNVBAMTC3RhcmlhZwucnRw
MQwwCgYDVQQHEwNSVFAxZARBgNVBAoTCKNpc2NvIEluYy4xCzAJBgNVBAGTAk5D
MQwwCgYDVQQLEwNUQUUMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5
gnqxG/GgDsxf0B7iWpNkCZpedKC5Qj5Up0EuMMx/OsAUXUNb1JNktGMmW7dq6p9Z
4zAoFRMgQFR3X1Vd6h3cMPWNghAeWGY1cMKMr5n2M3L9DdeLZ00D0ekCqTxG70D8
tFfJzgvhEQwVDj0zRjUk9yjmoeLx8GNgm4gB6v2QPm+fajNHbf91KRUFy9AHyMRs
a+DmpWcvzvFiyP28vSxAUIT3WMGJwwMxRcXOB/jF5V668caFN0A7tDyUt/6YCW1K
FeuCHaOGBRgFFp71Frsh5uZq1C70wE07cZP5Mm3AWjds3ZDvi/oJBn5nCR8HuvkD
VN06z9NVIE06gP564n6RAGMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEA0pN8fD+H
Wa7n+XTwAb1jyC7yrj9Ll08bc6Viy4bo1rS15DxqAkvtCqsK+xAhScX2j9hxq2
pHBp8D5wMEmSUR39Jw77HRWNKH1tUauIJUc3wE0eZ3b6p0UJA1NqenMBZJby7Hgw
0wV9X42JmDfwnBpWUW+rEyZhm0N9AATdgxmpFGvKIEiOM+fA0BKNxc7p0MMdcaBw
cQr/+bSFF3dwr8q8FAwS51RJ2cMQGpTZ2sLD54GbudpJqYUvJky1sYcn2USqpFn
```

WbhZArh0AQiSxolI+B6pgk/GE+50fNAB01IVqAYzzG41V76p17soBp6mXr7dx0GL

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

## Zugehörige Informationen

- [Installationsanforderungen für ESA-Zertifikate](#)
- [Installieren eines SSL-Zertifikats über die CLI auf einer ESA](#)
- [Neues PKCS#12-Zertifikat auf der Benutzeroberfläche der Cisco ESA hinzufügen/importieren](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.