

Réinitialiser un certificat sur un appareil de sécurité de la messagerie

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Renouveler un certificat](#)

[Mettre à jour le certificat via l'interface utilisateur graphique](#)

[Mettre à jour le certificat via la CLI](#)

[Informations connexes](#)

Introduction

Ce document décrit comment renouveler un certificat expiré sur le dispositif de sécurité de la messagerie Cisco (ESA).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.


Renouveler un certificat

Si vous avez un certificat expiré sur votre ESA (ou un certificat qui expire bientôt), vous pouvez simplement mettre à jour le certificat actuel :

1. Téléchargez le fichier de demande de signature de certificat (CSR).
2. Fournissez le fichier CSR à votre autorité de certification (CA) et demandez un certificat signé PEM (Privacy-Enhanced Mail) (X.509).
3. Mettez à jour votre certificat actuel via l'une des méthodes décrites dans les sections

mentionnées.

Mettre à jour le certificat via l'interface utilisateur graphique

 Remarque : ces étapes supposent que le certificat a été créé, envoyé et validé dans la configuration ESA. Si vous créez un nouveau certificat, n'oubliez pas d'envoyer et d'enregistrer le certificat sur l'appliance avant de télécharger le CSR.

Pour commencer, accédez à à partir Network > Certificates de l'interface utilisateur graphique de l'appliance. Ouvrez votre certificat et téléchargez le fichier CSR via le lien illustré dans l'image suivante. Si l'ESA est membre d'un cluster, vous devez vérifier les autres certificats membres du cluster et utiliser la même méthode pour chaque machine. Avec cette méthode, la clé privée reste sur l'ESA. La dernière étape consiste à faire signer le certificat par votre autorité de certification.

Voici un exemple :

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

- Téléchargez le fichier CSR sur votre ordinateur local, comme illustré dans l'image précédente.
- Fournissez le fichier CSR à votre autorité de certification et demandez un certificat X.509 formaté.
- Une fois que vous avez reçu le fichier PEM, importez le certificat via la section **Upload Signed Certificate**. Téléchargez également le certificat intermédiaire (s'il est disponible) dans la section facultative.
- Envoyez et validez les modifications.
- Revenez à la page principale Certificates (**Network > Certificates** from the GUI).
- Vérifiez que la nouvelle date d'expiration apparaît et que le certificat est **VALIDE/ACTIF**.
- Envoyez et validez les modifications.

Mettre à jour le certificat via la CLI

Vous pouvez également mettre à jour le certificat via l'interface de ligne de commande. Cette méthode semble plus intuitive, car les invites sont au format question/réponse.

Voici un exemple :

```
<#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
8caFNOA7tDyUt/6YCWlKFeuCHaOGBRgFFp71Frsh5uZq1C70wE07cZP5Mm3AWjds
3ZDvi/oJBn5nCR8HuvkDVNO6z9NVIE06gP564n6RAgMBAAEwDQYJKoZIhvcNAQEF
BQADggEBAA/BTYiw+OwAh1q3z1yfW6oVyx03/bGEdeTOTE8U3naBBKM/Niu8zAwK
7yS4tkkK3b96HK98IKWux0VSY0EiVw8EUWSa1k/2zsLEp5/iuZ/eAfdshRjDQKn3
H541MuowGaQc6NGtLjIfFet5pQ7w7R44z+4oSxYsT9FLH78/w5DdLf6Rk696c1p
hb9U9l7g7SnKvDrwLZ6i4Sn0TA6b1/z0p9DuvVSwwTNEHcn3kCbmbFpsD2Hd6EWD
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-----

MIIcPjCCAY4CAQAwYTELMAkGA1UEBhMCVVMxFDASBgNVBAMTC3RhcmlhZwucnRw
MQwwCgYDVQQLHEwNSVFAxZzARBGNVBAoTCkNpc2NvIE1uYy4xCzAJBgNVBAGTAK5D
MQwwCgYDVQQLLEwNUQUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5
gnqxG/GgDsxfOB7iWpNkCZpedKc5Qj5Up0EuMMx/OsAUXUNb1JNktGMmW7dq6p9Z
4zAoFRMgQFR3X1Vd6h3cMPWNgHAeWGY1cMKMr5n2M3L9DdeLZ00D0ekCqTxG70D8
tFfJzgvhEQwVDj0zRjUk9yjmoelx8GNgm4gB6v2QPm+fajNHbf91KRUFy9AHyMRs
a+DmpWcvzvFiyP28vSxAUIT3WMGJwwMxRcXOB/jF5V668caFNOA7tDyUt/6YCW1K
FeuCHaOGBRgFFp71Frsh5uZq1C70wE07cZP5Mm3AWjds3ZDvi/oJBn5nCR8HuvkD
VNO6z9NVIE06gP564n6RAGMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEAOpN8fd+H
Wa7n+XTwAb1jyC7yrjp9L1o8bc6Viy4bo1rS15DxqAkvtCqssK+xAAScX2j9hxq2
pHBp8D5wMEMSUR39Jw77HRWNKH1tUauIJUc3wEOeZ3b6pOUJA1NQenMBZJby7Hgw
0wV9X42JmDfwNBpWUW+rEyZHm0N9AATdgxmpFGvKIEiOM+FA0BKNxc7p0MMdcaBw
cQr/+bSFF3dwR8q8FAwS51RJ2cMQGpTZ2sLD54GbudpJqYUvjkylsYcn2USqupFn
WbhZArh0AQiSxo1I+B6pgk/GE+50fNAB01IVqAYzzG41V76p17soBp6mXr7dxOGL
YM21mN12Rq3BkQ==

-----END CERTIFICATE REQUEST-----

List of Certificates

Table with 5 columns: Name, Common Name, Issued By, Status, Remaining. Rows include tarheel.r, test, and Demo.

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

- [Installation des certificats ESA requise](#)
- [Installer un certificat SSL via l'interface de ligne de commande sur un ESA](#)
- [Ajout/importation d'un nouveau certificat PKCS#12 sur l'interface utilisateur graphique Cisco ESA](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.