Reinitialize a Certificate on an Email Security Appliance

Contents

Introduction

This document describes how to renew an expired certificate on the Cisco Email Security Appliance (ESA).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

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. If your network is live, ensure that you understand the potential impact of any command.

Renew a Certificate

If you have an expired certificate on your ESA (or one that expires soon), you can simply update the current certificate:

1. Download the Certificate Signing Request (CSR) file.
2. Provide the CSR file to your Certificate Authority (CA) and request a Privacy-Enhanced Mail (PEM) (X.509) signed certificate.
3. Update your current certificate via one of the methods that are described in the sections mentioned.

Update the Certificate via the GUI

Note: These steps assume the certificate has been created, submitted, and committed to the ESA

configuration. If you create a new certificate, remember to submit and save the certificate to the appliance before you download the CSR.

In order to begin, navigate to Network > Certificates from the appliance GUI. Open your certificate and download the CSR file via the link that is shown in the next image. If the ESA is a member of a cluster, you must verify the other cluster member certificates and use the same method for each machine. With this method, the private key remains on the ESA. The last step is to have the certificate signed by your CA.

Here is an example:

1. Download the CSR file to your local computer, as shown in the earlier image.
2. Provide the CSR file to your CA and request an X.509 formatted certificate.
3. Once you receive the PEM file, import the certificate via the **Upload Signed Certificate** section. Also, upload the intermediate certificate (if available) in the optional section.
4. Submit and commit the changes.
5. Return to the main Certificates page (**Network > Certificates** from the GUI).
6. Verify that the new expiration date appears and that the certificate shows as **VALID/ACTIVE**.
7. Submit and commit the changes.

Update the Certificate via the CLI

You can also update the certificate via the CLI. This method seems more intuitive, as the prompts are in question/answer format.

Here is an example:

```
<#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
7yS4tkWK3b96HK98IKWuxOVSYOEivW8EUWSalK/2zsLEp5/iuZ/eAfdsHrJdQKn3
H541MuowGaQc6NGtLjIfFet5pQ7w7R44z+4oSWXYsT9FLH78/w5DdLf6Rk696c1p
hb9U9lg7SnKvDrwLZ6i4Sn0TA6bl/z0p9DuvVSwWTNEHcn3kCbmbFpsD2Hd6EWKD
7OzXapUp6/xG79pc2gFXHfgORcmsozcmHPCjXjnL4OjpUExonSjffB3HhSKDqjhf
AOuN6Psgar9yz8M/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
tFfJzgvhEQwVDjOzRjUk9yjmoeLx8GNgm4gB6v2QPm+fajNHbf9lKRUFy9AHyMRs
a+DmpWcvzvFiyP28vSxAUIT3WMGJwwMxRcXOB/jF5V668caFNOA7tDyUt/6YCW1K
FeuCHaOGBRgFFp71Frsh5uZq1C7OwE07cZP5Mm3AWjds3ZDvi/oJBn5nCR8HuvkD
VNO6z9NVIEO6gP564n6RAgMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEAOpN8fD+H
Wa7n+XTwAb1jyC7yrjp9Llo8bc6Viy4bolrS15DxqAkvTCqssK+xhAScX2j9hxq2
pHBp8D5wMEmSUR39Jw77HRWNKHltUauIJUc3wEOeZ3b6pOUJAlNQenMBZJby7Hgw
OwV9X42JmDfwNBpWUW+rEyZHmON9AATdgxmpFGvKIeiOM+fAOBKNxc7pOMMdcaBw
cQr/+bSfF3dwR8q8FAwS51RJ2cMQGpTZ2sLD54GbudpJqYUvjky1sYcn2USqupFn
WbhzArhOAQiSxolI+B6pgk/GE+5OfNABOlIVqAYzzG41V76p17soBp6mXr7dxOGL
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

Related Information

- ESA Certificate Installation Requirements
- Install an SSL Certificate via the CLI on an ESA
- Add/Import New PKCS#12 Certificate on the Cisco ESA GUI
- Cisco Technical Support & Downloads