How to Generate and Install a Certificate on an SMA

Contents

Introduction

This document describes how to generate and install a certificate for configuration and use on a Cisco Security Management Appliance (SMA).

Prerequisites

You will need to have access to run the command **openssl** locally.

You will need admin account access to your Email Security Appliance (ESA), and admin access to the CLI of your SMA.

You must have these items available in .pem format:

- X.509 certificate
- Private key that matches your certificate
- Any intermediate certificates provided by your Certificate Authority (CA)

How to Generate and Install a Certificate on an SMA

> **Tip**: It is recommended to have a certificate signed by a trusted CA. Cisco does not recommend a specific CA. Depending on the CA you choose to work with, you may receive back the signed certificate, private key, and intermediate certificate (where applicable) in various formats. Please research or discuss directly with the CA the format of the file they provide to you prior to installing the certificate.

Currently, the SMA does not support generating a certificate locally. Instead, it is possible to

generate a self-signed certificate on the ESA. This can be used as a workaround to create a certificate for the SMA in order to be imported and configured.

Create and Export Certificate from an ESA

1. From the ESA GUI, create a self-signed certificate from **Network > Certificates > Add Certificate**. When creating the self-signed certificate, it is important for "Common Name (CN)" to use the hostname of the SMA and not of the ESA, so that the certificate can be properly used.
2. Submit and commit changes.
3. Export the certificate created from **Network > Certificates > Export Certificates**. You have two options, (1) export and save/use as self-signed certificate, or (2) download certificate signing request (if you are needing to have the certificate signed externally): Save/Use as a Self-Signed Certificate: Choose **Export Certificates**Give it a file name (e.g. mycert.pfx) and passphrase that will be used when converting the certificate.This will automatically prompt you to save the file locally.Proceed to "Convert the Exported Certificate".Download Certificate Signing Request **Network > Certificates**Click on the certificate name you created.In the "Signature Issued By" section, click **Download Certificate Signing Request...**Save the .pem file locally and submit to the CA.

Convert the Exported Certificate

The certificate created and exported from the ESA will be in .pfx format. The SMA only supports .pem format for importing, so this certificate will need to be converted. In order to convert a certificate from .pfx format to .pem format, please use the following **openssl** command example:

```
openssl pkcs12 -in mycert.pfx -out mycert.pem -nodes
```

You will be prompted for the passphrase used while creating the certificate from the ESA. The .pem file created in the OpenSSL command will contain both the certificate and the key in .pem format. The certificate is now ready to be configured on the SMA. Please proceed to "Install the Certificate" section of this article.

Create Certificate with OpenSSL

Alternatively, if you have local access to run **openssl** from your PC/workstation, you can issue the following command to generate the certificate and save the needed .pem file and private key into two separate files:

```
openssl req -newkey rsa:2048 -new -nodes -x509 -days 3650 -keyout sma_key.pem -out sma_cert.pem
```

The certificate is now ready to be configured on the SMA. Please proceed to "Install the Certificate" section of this article.

Additional Option, Exporting a Certificate from an ESA

Instead of converting the certificate from .pfx into .pem, as mentioned above, you can save a configuration file without masking the passwords on the ESA. Open the saved ESA .xml configuration file and search for the <certificate> tag. The certificate and private key will be already

in .pem format. Copy the certificate and private key for importing the same into the SMA as described "Install the Certificate" section below.

> **Note**: This option is only valid for appliances running AsyncOS 11.1 and older, where the configuration file can be saved using the 'plain passphrase' option. Newer versions of AsyncOS provide only the option to mask passphrase or encrypt passphrase. Both options encrypt the private key, which is needed for the certificate import or paste option.

> **Note**: If you did opt for #2 above, "Download Certificate Signing Request", and have the certificate signed by a CA, you will need to import the signed certificate back to the ESA the certificate was created from prior to saving the configuration file for making a copy of the certificate and private key. Import can be done by clicking on the certificate name on ESA GUI and use the option " Upload Signed Certificate".

Install the Certificate on the SMA

A single certificate can be used for all services, or an individual certificate can be used for each of the four services:

- Inbound TLS
- Outbound TLS
- HTTPS
- LDAPS

On the SMA, log into via the CLI and complete the following steps:

1. Run **certconfig**.
2. Choose the **setup** option.
3. You will need to choose whether to use the same certificate for all services or to use separate certificates for each individual service: When presented "Do you want to use one certificate/key for receiving, delivery, HTTPS management access, and LDAPS?", answering "Y" will only require you to enter the certificate and key once, and will then assign that certificate to all services.If you choose to enter "N", you will need to enter in the certificate, key, and intermediate certificate (where applicable) for each service when prompted: Inbound, Outbound, HTTPS, and Management
4. When prompted, paste the certificate or key.
5. End with '.' on its own line for each entry in order to indicate that you are done pasting the current item. (See the "Example" section.)
6. If you have an intermediate certificate, be sure to enter it when prompted to do so.
7. Once completed, press **Enter** to return to the main CLI prompt of the SMA.
8. Run **commit** to saving the configuration.

> **Note**: Do not exit the **certconfig** command with Ctrl+C since this immediately cancels your changes.

Example

```
mysma.local> certconfig

Currently using the demo certificate/key for receiving, delivery, HTTPS management access, and
LDAPS.


Choose the operation you want to perform:
- SETUP - Configure security certificates and keys.
[]> setup

Do you want to use one certificate/key for receiving, delivery, HTTPS management access, and
LDAPS? [Y]> y

paste cert in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAwIJAIXvIlkArow9MA0GCSqGSIb3DQEBBQUAMG4xCzAJBgNV
BAYTAlVTMRowGAYDVQQDDBF3dS5jYWxvLmNpc2NvLmNvbTEMMAoGA1UEBwwDUlRQ
MQ4wDAYDVQQKDAVDaXNjbzEXMBUGA1UECAwOTm9ydGggQ2Fyb2xpbmExDDAKBgNV
BAsMA1RBQzAeFw0xNzExMTAxNjA3MTRaFw0yNzExMDgxNjA3MTRaMG4xCzAJBgNV
BAYTAlVTMRowGAYDVQQDDBF3dS5jYWxvLmNpc2NvLmNvbTEMMAoGA1UEBwwDUlRQ
MQ4wDAYDVQQKDAVDaXNjbzEXMBUGA1UECAwOTm9ydGggQ2Fyb2xpbmExDDAKBgNV
BAsMA1RBQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKPz0perw3QA
ZH8xctOrvvjsnOPkItmSc+DUqtVKM6OOOkNHA2WY9XJ3+vESwkIdwexibj6VUQ85
K7NE6zOgRfpYdQsxmpIWhzYf9qCBOXuKsRw/9jonKk98DfHFM02J3BSmmgZ0MPp7
6EwA/sZAN+aqYB7IE1fgnqpEXek8xFlfcVnS2YTc7NXz78lNK0jvXOtCVBrWFu0z
lEmZVpAj0AKkz1nujvzfOqEzed+tjauZr7nDIaiTrzhLKte4pJUm3T61q/PhegvN
Iy/WHN1xojP+FzjRAUlmtmjMzHyM2///dmq8JivUlaLXX9vUfdK3VViIOIz4zngG
Rz85QXO7ivcCAwEAATANBgkqhkiG9w0BAQUFAAOCAQEAM10zCcOOtqV1LDBmoDqd
4G2IhVbBESsbvZ/QmB6kpikT4pe5clQucskHq4D/xg1EZyfuXu+4auMie4B9Dym8
8pjbMDDi9hJPZ7j85nWMd6SfWhQUOPankdazpCycN6gNVzRBgPdR8tLOvt90vtV4
KCPmDYbwi6kfOl8tvjWHMh/wYicfvFRy0vPMpemtbCVGyC3cpquv8nFDutB6exym
skotn5wixCqErKlnHdUa3Z+zhutIAm/Q0sVWQQlbZZ+MIxBegyJ0ucTmBqqQHhhJ
pSO7PbevxwanYVXvNR8o2feAWs5LYkrwqdGRxLJmHjFnMV3PbkwRPgFWQ6AD1g12
34==
-----END CERTIFICATE-----
.
paste key in PEM format (end with '.'):
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCj89KXq8N0AGR/
MXLTq7747Jzj5CLZknPg1KrVSjOjjjpDRwNlmPVyd/rxEsJCHcHsYm4+lVEPOSuz
ROszoEX6WHULMZqSFoc2H/aggTl7irEcP/Y6JypPfA3xxTNNidwUppoGdDD6e+hM
AP7GQDfmqmAeyBNX4J6qRF3pPMRZX3FZ0tmE3OzV8+/JTStI71zrQlQa1hbtM5RJ
mVaQI9ACpM9Z7o783zqhM3nfrY2rma+5wyGok684SyrXuKSVJt0+tavz4XoLzSMv
1hzdcaIz/hc40QFJZrZozMx8jNv//3ZqvCYr1JWi11/b1H3St1VYiDiM+M54Bkc/
OUFzu4r3AgMBAAECggEAB9EFjsaZHGwyXmAIpe/PvIVnW3QSd0YEsUjiViXh/V+4
BmIZ1tuqhAkVVS38RfOuPatZrzEmOrASlcro3b6751oVRnHYeTOKwblXZEKU739m
vz6Lai1Y1o5HCepJbl5uuCtTN5CNjzueERWRD/ma0Kv5xi3qwitK1TpKMeb8Q3h2
YABmpk0TyJQ5ixLw3ch9ru1nqiO5zQ91GvIuDckudUu/bBnao+jV7D362lIPyLG8
03GqNviNZ6c3wjD0yQWg619g+ZmjM8DTtDR16zmzBvQ4TgZi22sUWrSSILRa69jW
q8XszQVRydl+gt666iUeN/ozmEMt5J8pu3i9vf3G2QKBgQDHyfv55rjZbWyf0eAT
Ch5T1YsjjMgMOtC9ivi5mMQCunWyRiyZ6qqSBME9Tper/YdAA07PoNtTpVPYyuVX
DDmyuWGHE04baf5QEmSgvQjXOSUPN5TI9hc5/mtvD8QjDO6rebUWxV3NJoR7YNrz
OmfARMXxaF+/mEj+6blSjZuGaQKBgQDSFKvYownPL6qTFhIH7B3kOLwZHk6cJUau
Zoaj7vTw7LrVJv1B0iLPmttEXeJgxzlFYR8tzfn0kTxGQlnhQxXkQ1kdDeqaiLvm
0TtmHMDupjDNKCNH8yBPqB+BIA4cB+/vo23W1HMHpGgqYWRRX/qremL72XFZSRnM
B8nRwK4aXwKBgB+hkwtVxB5ofLIxAFEDYRnUzVqrh2CoTzQzNH3t+dqUut2mzpjv
1mGX7yBNuSW51hgEbg3hYdg0bLn+JaFKhjgNsas5Gzyr41+6CcSJKUUp/vwRyLSo
gbTk2w2SaXNDMOZlNo6MYPWCC6edBg1MSfDe8pft9nrXGXeCeZzgXqdBAoGAQ6Iq
DQ24O76h0Ma7OVe36+CkFgYe0sBheAZD9IUa0HG2WKc7w7QORv4Y93KuTe/1rTNu
```

```
YUW94hHb8Natrwr1Ak74YpU3YVcB/3Z/BAnfxzUz4ui4KxLH5T1AH0cdo8KeaW0Z
EJ/HBL/WVUaTkGsw/YHiWiiQCGmzZ29edyvsIUsCgYEAvJtx0ZBAJ443WeHajZWm
J2SLKy0KHeDxZOZ4CwF5sRGsmMofILbK0OuHjMirQ5U9HFLpcINt11VWwhOiZZ5l
k6o79mYhfrTMa4LlHOTyScvuxELqow82vdj6gqX0HVj4fUyrrZ28MiYOMcPw6Y12
34VjKaAsxgZIgN3LvoP7aXo=
-----END PRIVATE KEY-----
.
Do you want to add an intermediate certificate? [N]> n

Currently using one certificate/key for receiving, delivery, HTTPS management access, and LDAPS.


Choose the operation you want to perform:
- SETUP - Configure security certificates and keys.
- PRINT - Display configured certificates/keys.
- CLEAR - Clear configured certificates/keys.
[]>

mysma.local> commit

Please enter some comments describing your changes:
[]> Certificate installation

Changes committed: Fri Nov 10 11:46:07 2017 EST
```

Verify the Imported and Configured Certificate on the SMA

1. Connect to the SMA via GUI using HTTPS (https://<SMA IP or hostname>) and enter your log-in credentials.
2. Next to the URL in the address bar on your browser, click the lock icon or information icon to check the validity of the certificate, expiry, etc. Depending on which browser you are using, your actions and results may vary.
3. Click on the Certification Path to check the chain of certificates.

Related Information

- **Technical Support & Documentation - Cisco Systems**