# Comment générer et installer un certificat sur un SMA

## Contenu



## Introduction

Ce document décrit comment générer et installer un certificat pour configuration et utilisation sur un dispositif de gestion de la sécurité Cisco (SMA).

## Conditions préalables

Vous devez avoir accès pour exécuter la commande **openssl** localement.

Vous aurez besoin d'un accès de compte d'administrateur à votre appliance de sécurité de la messagerie (ESA) et d'un accès d'administrateur à l'interface de ligne de commande de votre SMA.

Vous devez disposer de ces éléments au format .pem :

- Certificat X.509
- Clé privée correspondant à votre certificat
- Tout certificat intermédiaire fourni par votre autorité de certification (CA)

## Comment générer et installer un certificat sur un SMA

> **Astuce** : Il est recommandé d'avoir un certificat signé par une autorité de certification de confiance. Cisco ne recommande pas une autorité de certification spécifique.  Selon l'autorité de certification avec laquelle vous choisissez de travailler, vous pouvez recevoir le certificat signé, la clé privée et le certificat intermédiaire (le cas échéant) dans différents formats.  Veuillez rechercher ou discuter directement avec l'AC le format du fichier qu'il vous fournit avant d'installer le certificat.

Actuellement, le SMA ne prend pas en charge la génération locale d'un certificat.  Au lieu de cela, il est possible de générer un certificat auto-signé sur l'ESA. Ceci peut être utilisé comme solution de contournement pour créer un certificat pour le SMA afin d'être importé et configuré.

## Créer et exporter un certificat à partir d'un ESA

1. Àpartir de l'interface graphique de l'ESA, créez un certificat auto-signé à partir de **Network > Certificates > Add Certificate**. Lors de la création du certificat auto-signé, il est important que « Common Name (CN)" utilise le nom d'hôte du SMA et non du ESA, afin que le certificat puisse être correctement utilisé.
2. Envoyez et validez les modifications.
3. Exporter le certificat créé à partir de **Network > Certificates > Export Certificates**.  Vous disposez de deux options : (1) exporter et enregistrer/utiliser en tant que certificat auto-signé, ou (2) télécharger une demande de signature de certificat (si vous devez faire signer le certificat en externe) : Enregistrer/utiliser en tant que certificat auto-signé : Choisissez **Exporter les certificats**Donnez-lui un nom de fichier (par exemple mycert.pfx) et une phrase de passe qui seront utilisés lors de la conversion du certificat.Cela vous invite automatiquement à enregistrer le fichier localement.Passez à Convertir le certificat exporté.Télécharger la demande de signature de certificat **Réseau > Certificats**Cliquez sur le nom du certificat que vous avez créé.Dans la section Signature émise par, cliquez sur **Télécharger la demande de signature de certificat...**Enregistrez le fichier .pem localement et envoyez-le à l'Autorité de certification.

### Convertir le certificat exporté

Le certificat créé et exporté à partir de l'ESA sera au format .pfx. Le SMA ne prend en charge que le format .pem pour l'importation, de sorte que ce certificat devra être converti.  Afin de convertir un certificat du format .pfx au format .pem, utilisez l'exemple de commande **openssl** suivant :

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

Vous serez invité à saisir la phrase de passe utilisée lors de la création du certificat à partir de l'ESA.  Le fichier .pem créé dans la commande OpenSSL contient le certificat et la clé au format .pem.  Le certificat est maintenant prêt à être configuré sur le SMA.  Veuillez passer à la section « Installer le certificat » de cet article.

## Créer un certificat avec OpenSSL

Sinon, si vous disposez d'un accès local pour exécuter **openssl** à partir de votre PC/station de travail, vous pouvez émettre la commande suivante pour générer le certificat et enregistrer le fichier .pem et la clé privée nécessaires dans deux fichiers distincts :

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

Le certificat est maintenant prêt à être configuré sur le SMA.  Veuillez passer à la section « Installer le certificat » de cet article.

## Option supplémentaire, Exportation d'un certificat d'un ESA

Au lieu de convertir le certificat de .pfx en .pem, comme mentionné ci-dessus, vous pouvez enregistrer un fichier de configuration sans masquer les mots de passe sur le ESA. Ouvrez le fichier de configuration ESA .xml enregistré et recherchez la balise <certificat>. Le certificat et la clé privée seront déjà au format .pem. Copiez le certificat et la clé privée pour l'importation dans le SMA, comme décrit dans la section Installer le certificat ci-dessous.

> **Note**: Cette option n'est valide que pour les appliances exécutant AsyncOS 11.1 et versions ultérieures, où le fichier de configuration peut être enregistré à l'aide de l'option de phrase de passe simple. Les nouvelles versions d'AsyncOS offrent uniquement la possibilité de masquer la phrase de passe ou de chiffrer la phrase de passe. Les deux options chiffrent la clé privée, nécessaire pour l'option d'importation ou de collage de certificat.

> **Note**: Si vous avez opté pour le numéro 2 ci-dessus, « Télécharger la demande de signature de certificat », et que le certificat est signé par une autorité de certification, vous devez importer le certificat signé à nouveau dans l'ESA à partir duquel le certificat a été créé avant d'enregistrer le fichier de configuration pour faire une copie du certificat et de la clé privée. L'importation peut être effectuée en cliquant sur le nom du certificat sur l'interface graphique de l'ESA et en utilisant l'option " Upload Signed Certificate « .

## Installer le certificat sur SMA

Un seul certificat peut être utilisé pour tous les services, ou un certificat individuel peut être utilisé pour chacun des quatre services :

- TLS entrant
- TLS sortant
- HTTPS
- LDAPS

Sur le SMA, connectez-vous via l'interface de ligne de commande et procédez comme suit :

1. Exécutez **certconfig**.
2. Sélectionnez l'option **de configuration**.
3. Vous devez choisir d'utiliser le même certificat pour tous les services ou des certificats distincts pour chaque service : Lorsqu'il est présenté « Voulez-vous utiliser un certificat/une clé pour la réception, la livraison, l'accès à la gestion HTTPS et le LDAPS ? », la réponse « Y » ne vous demandera de saisir le certificat et la clé qu'une seule fois, puis attribuera ce certificat à tous les services.Si vous choisissez d'entrer « N », vous devez entrer dans le certificat, la clé et le certificat intermédiaire (le cas échéant) pour chaque service lorsque vous y êtes invité : Entrantes, sortantes, HTTPS et gestion
4. Lorsque vous y êtes invité, collez le certificat ou la clé.
5. Terminer par '.' sur sa propre ligne pour chaque entrée afin d'indiquer que vous avez terminé de coller l'élément actif. (Voir la section « Exemple ».)
6. Si vous disposez d'un certificat intermédiaire, assurez-vous de le saisir lorsque vous y êtes invité.

7. Une fois terminé, appuyez sur **Entrée** pour revenir à l'invite CLI principale de la SMA.
8. Exécutez **commit** pour enregistrer la configuration.

**Remarque** : Ne quittez pas la commande **certconfig** avec Ctrl+C, car cela annule immédiatement vos modifications.

# Exemple

```
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
```

# Vérifier le certificat importé et configuré sur SMA

1. Connectez-vous au SMA via l'interface utilisateur graphique à l'aide du protocole HTTPS (https://<IP SMA ou nom d'hôte>) et saisissez vos informations d'identification de connexion.
2. En regard de l'URL dans la barre d'adresse de votre navigateur, cliquez sur l'icône de verrouillage ou l'icône d'information pour vérifier la validité du certificat, l'expiration, etc. Selon le navigateur que vous utilisez, vos actions et vos résultats peuvent varier.
3. Cliquez sur le chemin de certification pour vérifier la chaîne de certificats.

# Informations connexes

- Support et documentation techniques - Cisco Systems