Configurer CSR pour CMS avec OpenSSL pour le chiffrement

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Composants utilisés](#)

[Configurer](#)

[Vérifier](#)

Introduction

Ce document décrit comment créer des certificats pour Cisco Meeting Server (CMS) avec Open Secure Sockets Layer (OpenSSL).

Contribution de Moises Martinez, ingénieur du centre d'assistance technique Cisco.

Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Ouvrez SSL.
- Configuration de CMS.

Composants utilisés

Les informations contenues dans ce document sont basées sur les logiciels suivants :

- OpenSSL Light 1.1

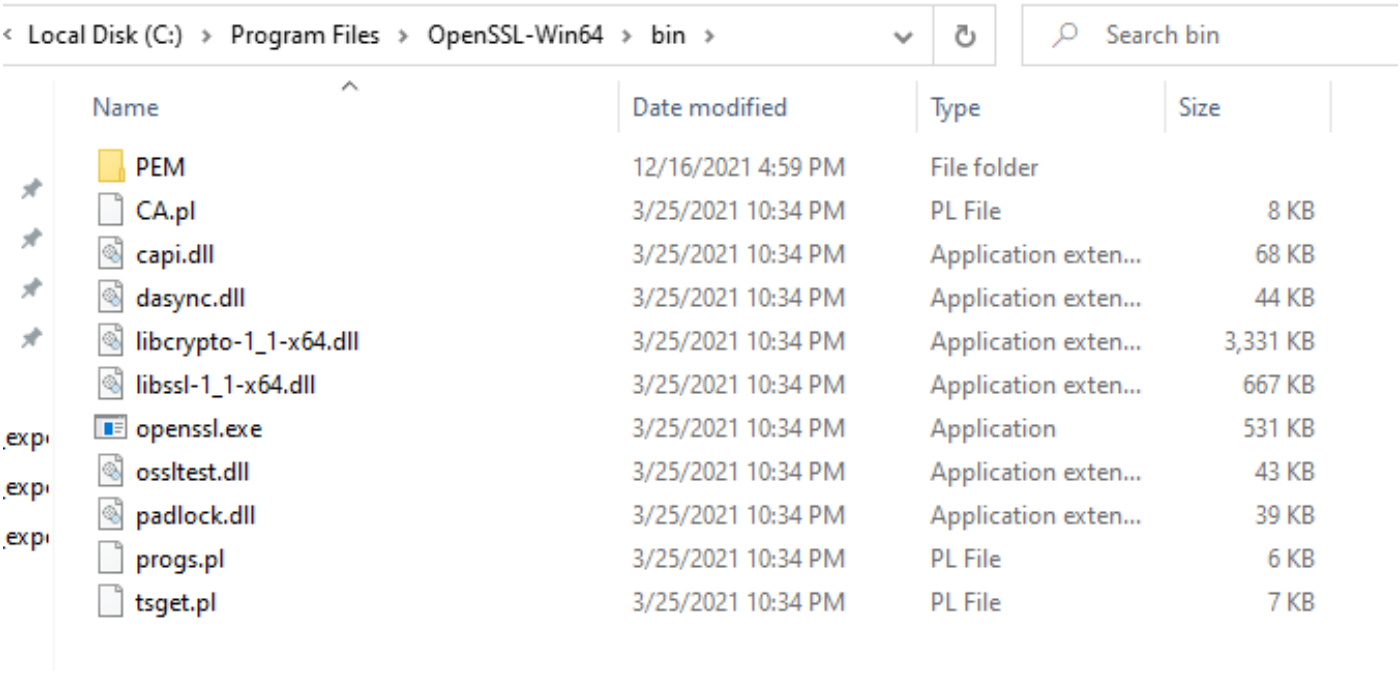
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer

Étape 1. Téléchargez OpenSSL Light 1.1.

Étape 2. Installer OpenSSL sur votre ordinateur

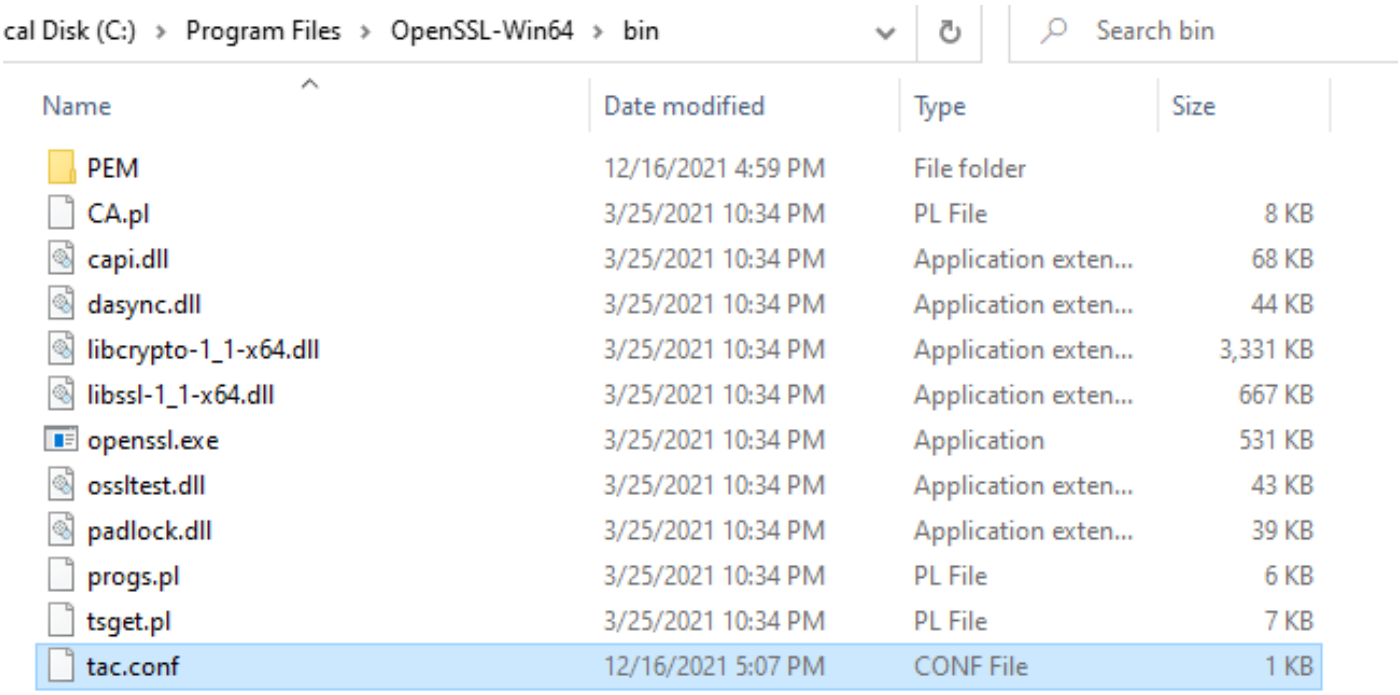
Étape 3. Accédez au dossier dans lequel SSL a été installé. En général, il est installé sur C:\Program Files\OpenSSL-Win64\bin.



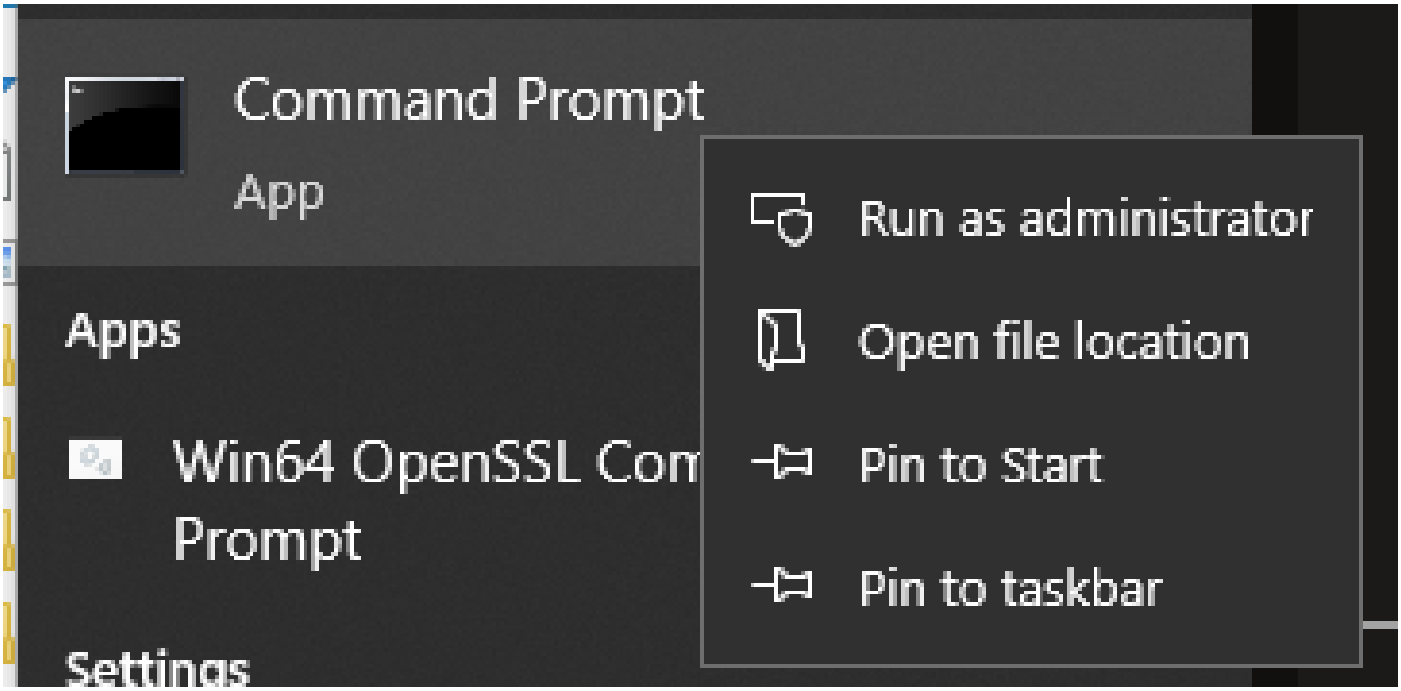
Étape 4. Ouvrez le Bloc-notes et entrez les informations requises pour la demande de signature de certificat (CSR), comme indiqué dans l'exemple suivant :

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no
[req_distinguished_name]
C = US
ST = California
L = San Jose
O = TAC
OU = IT
CN = cms.tac.cisco.com
[v3_req]
extendedKeyUsage = serverAuth, clientAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = webbridge3.tac.cisco.com
DNS.2 = webadmin.tac.cisco.com
DNS.3 = xmpp.tac.cisco.com
```

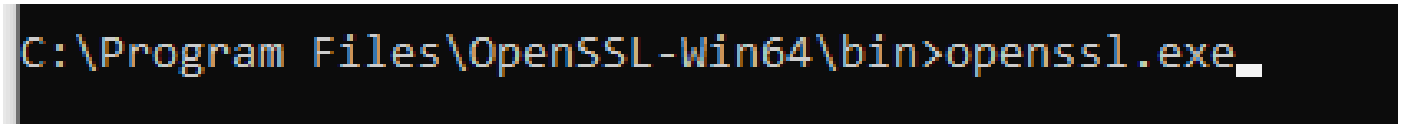
Étape 5. Une fois les informations saisies pour le CSR, ce fichier est enregistré sous le nom tac.conf dans le chemin suivant : C:\Program Files\OpenSSL-Win64\bin.



Étape 6. Ouvrez l'invite de commandes sur le PC et sélectionnez Exécuter en tant qu'administrateur.



Étape 7. Accédez au chemin d'accès où le fichier est stocké via l'invite de commandes, entrez la commande openssl.exe et sélectionnez Entrée.



Étape 8. Exécutez la commande suivante : req -new -newkey rsa : 4096 - nodes -keyout cms.key -out cms.csr -config tac.conf.

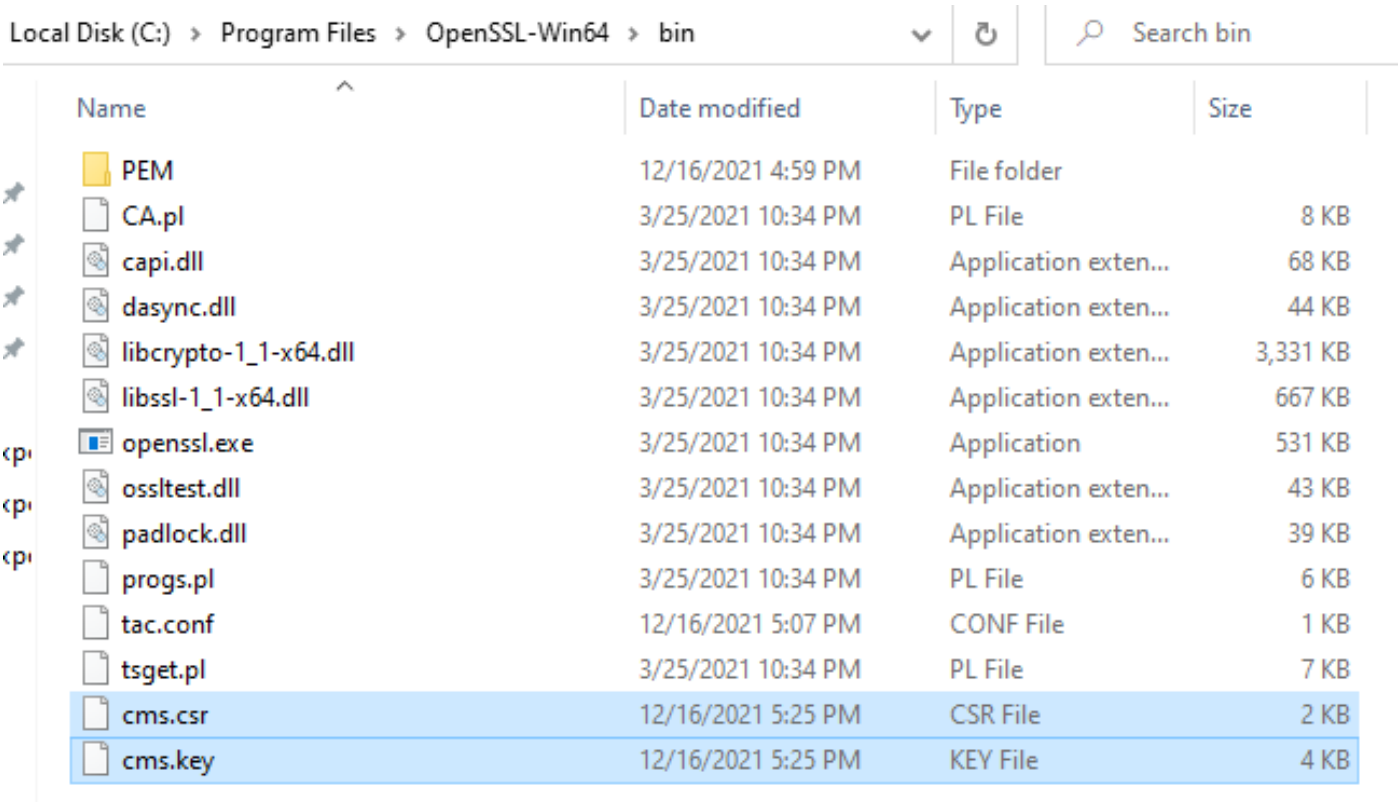
```
C:\Program Files\OpenSSL-Win64\bin>openssl.exe
OpenSSL> req -new -newkey rsa:4096 -nodes -keyout cms.key -out cms.csr -config tac.conf
```

```
C:\Program Files\OpenSSL-Win64\bin>openssl.exe
OpenSSL> req -new -newkey rsa:4096 -nodes -keyout cms.key -out cms.csr -config tac.conf
Generating a RSA private key
.....................................................++++
.....................................................................................................
writing new private key to 'cms.key'
-----
```

Vérifier

Si aucune erreur n'est affichée, deux nouveaux fichiers sont générés dans le même dossier :

- cms.key
- cms.csr



Ce nouveau fichier cms.csr peut être signé par une autorité de certification (CA).

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.