

암호화를 위해 OpenSSL을 사용하여 CMS용 CSR 구성

목차

[소개](#)

[사전 요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[다음을 확인합니다.](#)

소개

이 문서에서는 OpenSSL(Secure Sockets Layer)을 사용하는 Cisco CMS(Meeting Server)용 인증서를 생성하는 방법에 대해 설명합니다.

기고자: Cisco TAC 엔지니어 Moises Martinez

사전 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SSL을 엽니다.
- CMS 컨피그레이션

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어를 기반으로 합니다.

- OpenSSL Light 1.1

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

1단계. OpenSSL Light 1.1을 다운로드합니다.

2단계. 컴퓨터에 OpenSSL을 설치합니다.

3단계. SSL이 설치된 폴더로 이동합니다. 일반적으로 C:\Program Files\OpenSSL-Win64\bin에 설치됩니다.

< Local Disk (C:) > Program Files > OpenSSL-Win64 > bin >

Name	Date modified	Type	Size
PEM	12/16/2021 4:59 PM	File folder	
CA.pl	3/25/2021 10:34 PM	PL File	8 KB
capi.dll	3/25/2021 10:34 PM	Application exten...	68 KB
dasync.dll	3/25/2021 10:34 PM	Application exten...	44 KB
libcrypto-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	3,331 KB
libssl-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	667 KB
openssl.exe	3/25/2021 10:34 PM	Application	531 KB
ossltest.dll	3/25/2021 10:34 PM	Application exten...	43 KB
padlock.dll	3/25/2021 10:34 PM	Application exten...	39 KB
progs.pl	3/25/2021 10:34 PM	PL File	6 KB
tsget.pl	3/25/2021 10:34 PM	PL File	7 KB

4단계. 메모장을 열고 다음 예와 같이 CSR(Certificate Signing Request)에 필요한 정보를 입력합니다.

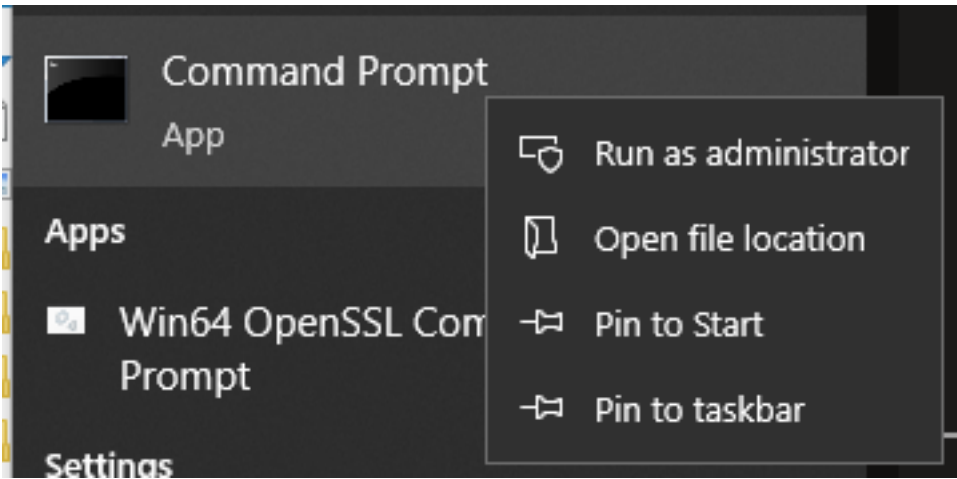
```
[req] distinguished_name = req_distinguished_name req_extensions = v3_req prompt = no
[req_distinguished_name] C = US ST = California L = San Jose O = TAC OU = IT CN =
cms.tac.cisco.com [v3_req] extendedKeyUsage = serverAuth, clientAuth subjectAltName = @alt_names
[alt_names] DNS.1 = webbridge3.tac.cisco.com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

5단계. CSR에 대한 정보를 입력하면 이 파일은 다음 경로에 **tac.conf**로 저장됩니다. C:\Program Files\OpenSSL-Win64\bin.

cal Disk (C:) > Program Files > OpenSSL-Win64 > bin

Name	Date modified	Type	Size
PEM	12/16/2021 4:59 PM	File folder	
CA.pl	3/25/2021 10:34 PM	PL File	8 KB
capi.dll	3/25/2021 10:34 PM	Application exten...	68 KB
dasync.dll	3/25/2021 10:34 PM	Application exten...	44 KB
libcrypto-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	3,331 KB
libssl-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	667 KB
openssl.exe	3/25/2021 10:34 PM	Application	531 KB
ossltest.dll	3/25/2021 10:34 PM	Application exten...	43 KB
padlock.dll	3/25/2021 10:34 PM	Application exten...	39 KB
progs.pl	3/25/2021 10:34 PM	PL File	6 KB
tsget.pl	3/25/2021 10:34 PM	PL File	7 KB
tac.conf	12/16/2021 5:07 PM	CONF File	1 KB

6단계. PC에서 Command Promt(명령 프롬프트)를 열고 Run as administrator(관리자로 실행)를 선택합니다.



7단계. 명령 프롬프트를 통해 파일이 저장되는 경로로 이동하고 명령 `openssl.exe`를 입력하고 `enter`를 선택합니다.

```
C:\Program Files\OpenSSL-Win64\bin>openssl.exe
```

8단계. 다음 명령을 실행합니다. `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'
-----
```

다음을 확인합니다.

오류가 표시되지 않으면 동일한 폴더에 두 개의 새 파일이 생성됩니다.

- cms 키
- cms.csr



Name	Date modified	Type	Size
PEM	12/16/2021 4:59 PM	File folder	
CA.pl	3/25/2021 10:34 PM	PL File	8 KB
capi.dll	3/25/2021 10:34 PM	Application exten...	68 KB
dasync.dll	3/25/2021 10:34 PM	Application exten...	44 KB
libcrypto-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	3,331 KB
libssl-1_1-x64.dll	3/25/2021 10:34 PM	Application exten...	667 KB
openssl.exe	3/25/2021 10:34 PM	Application	531 KB
ossltest.dll	3/25/2021 10:34 PM	Application exten...	43 KB
padlock.dll	3/25/2021 10:34 PM	Application exten...	39 KB
progs.pl	3/25/2021 10:34 PM	PL File	6 KB
tac.conf	12/16/2021 5:07 PM	CONF File	1 KB
tsget.pl	3/25/2021 10:34 PM	PL File	7 KB
cms.csr	12/16/2021 5:25 PM	CSR File	2 KB
cms.key	12/16/2021 5:25 PM	KEY File	4 KB

이 새 파일 **cms.csr**은 CA(Certificate Authority)에서 서명할 수 있습니다.