

使用OpenSSL為加密配置CMS的CSR

目錄

[簡介](#)

[必要條件](#)

[採用元件](#)

[設定](#)

[驗證](#)

簡介

本文說明如何使用開放安全套接字層(OpenSSL)為思科會議伺服器(CMS)建立證書。

作者：Moises Martinez，思科TAC工程師。

必要條件

思科建議您瞭解以下主題：

- 開啟SSL。
- CMS配置。

採用元件

本檔案中的資訊是根據以下軟體：

- OpenSSL精簡版1.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

步驟1. 下載OpenSSL Light 1.1。

步驟2. 在電腦上安裝OpenSSL。

步驟3. 導航到安裝SSL的資料夾。通常安裝在C:\Program Files\OpenSSL-Win64\bin上。

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

步驟4.開啟記事本，並輸入憑證簽署請求(CSR)所需的資訊，如下例所示：

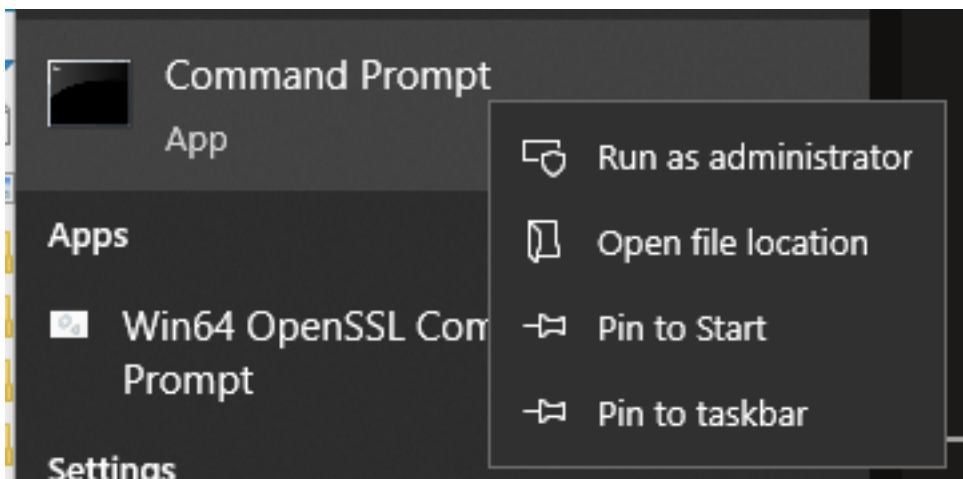
```
[req] distinguished_name = req_distinguished_name req_extensions = v3_req prompt = no
[req_distinguished_name] C = US ST = California L = San Jose O = TAC OU = IT CN =
cms.tac.cisco.com [v3_req] extendedKeyUsage = serverAuth, clientAuth subjectAltName = @alt_names
[alt_names] DNS.1 = webbridge3.tac.cisco.com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

步驟5.一旦為CSR輸入資訊，此檔案就會儲存在tac.conf的下一個路徑中：**C:\Program Files\OpenSSL-Win64\bin**。

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

步驟6.在PC上開啟Command Prompt，然後選擇Run as administrator。



步驟7.透過命令提示導航至儲存檔案的路徑，輸入`openssl.exe`指令，然後選擇enter。

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

步驟8.執行下一個命令：`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'
-----
```

驗證

如果未顯示錯誤，則會在同一資料夾中生成兩個新檔案：

- `cms.key`
- `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

此新檔案cms.csr可由憑證授權單位(CA)簽署。