

CSM — 如何為GUI訪問安裝第三方SSL證書

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[從使用者介面建立CSR](#)

[身份證書上傳到CSM伺服器](#)

簡介

思科安全管理器(CSM)提供使用第三方證書頒發機構(CA)頒發的安全證書的選項。當組織策略阻止使用CSM自簽名證書或要求系統使用從特定CA獲得的證書時，可以使用這些證書。

TLS/SSL將這些證書用於CSM伺服器 and 客戶端瀏覽器之間的通訊。本文說明在CSM中生成憑證簽署請求(CSR)的步驟，以及如何在同一中安裝身分和根CA憑證。

必要條件

需求

思科建議您瞭解以下主題：

- 瞭解SSL憑證架構。
- 思科安全管理器基礎知識。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全管理器4.11版及更高版本。

從使用者介面建立CSR

本節說明如何產生CSR。

步驟1.運行Cisco Security Manager首頁並選擇**Server Administration > Server > Security > Single-Server Management > Certificate Setup**。

步驟2.輸入下表所述欄位所需的值：

欄位	使用說明
國家/地區名稱	兩個字元的國家/地區代碼。
州或省	兩個字元的省/市/自治區代碼或省/市/自治區完整名稱。

- 地區 兩個字元的城市或城鎮代碼或城鎮的完整名稱。
- 組織名稱 組織的完整名稱或縮寫。
- 組織單位名稱 部門的完整名稱或縮寫。
- 電腦的DNS名稱、IP地址或主機名。
- 伺服器名稱 輸入具有正確且可解析的域名的伺服器名稱。這顯示在您的證書上（無論是自簽名還是第三
不應提供本地主機或127.0.0.1。
- 電子郵件地址 必須將郵件傳送到的電子郵件地址。

Self Signed Certificate Setup

Country Name:

State or Province:

City (Eg : SJ):

Organization Name:

Organization Unit Name:

Server Name*:

Email Address:

Certificate Bit: 2048

Note:
Server Name (Hostname or IP Address or FQDN) is the mandatory field. This is required to create the certificate. Ensure that the server name is same as the peer hostname that is used for setting up peer relations. Entering other fields are optional. However, it is desirable to provide all input fields for certificate regeneration.

步驟3.按一下Apply以建立CSR。

該過程生成以下檔案：

- server.key — 伺服器的私鑰。
- server.crt — 伺服器的自簽名證書。
- server.pk8 - PKCS#8格式的伺服器私鑰。
- server.csr — 證書簽名請求(CSR)檔案。

註：這是生成的檔案的路徑。

```
~CSCOp\MDC\Apache\conf\ssl\chain.cer  
~CSCOp\MDC\Apache\conf\ssl\server.crt  
~CSCOp\MDC\Apache\conf\ssl\server.csr  
~CSCOp\MDC\Apache\conf\ssl\server.pk8  
~CSCOp\MDC\Apache\conf\ssl\server.key
```

註：如果證書是自簽名證書，則無法修改此資訊。

身份證書上傳到CSM伺服器

本節介紹如何將CA提供的身份證書上傳到CSM伺服器

步驟1 查詢此位置可用的SSL實用程式指令碼

NMSROOT\MDC\Apache

注意:NMSROOT必須替換為CSM的安裝目錄。

此實用程式具有以下選項。

編號 選項

1 顯示伺服器證書資訊

它的作用.....

- 顯示CSM伺服器的證書詳細資訊。

對於第三方頒發的證書，此選項顯示伺服器證書、中間證書（如果有）

- 驗證證書是否有效。

此選項接受證書作為輸入，並且：

2 顯示輸入證書資訊

- 驗證憑證是否採用編碼的X.509憑證格式。

- 顯示證書的主題和頒發證書的詳細資訊。

- 驗證證書在伺服器上是否有效。

3 顯示伺服器信任的根CA證書

生成所有根CA證書的清單。

驗證是否可上傳由第三方CA頒發的伺服器證書。

選擇此選項時，實用程式：

- 驗證證書是否為Base64 Encoded X.509Certificate格式。

- 驗證證書在伺服器上是否有效

- 驗證伺服器私鑰和輸入伺服器證書是否匹配。

- 驗證是否可以將伺服器證書跟蹤到所需的根CA證書（已使用該證書）

- 如果也提供了中間鏈，則構建證書鏈，並驗證該鏈是否以正確的格式

4 驗證輸入憑證或憑證鏈結

驗證成功完成後，系統會提示您將憑證上傳到CSM伺服器。

實用程式顯示一個錯誤：

- 如果輸入證書不是所需的格式

- 如果證書日期無效或證書已過期。

- 如果無法驗證伺服器證書，或無法跟蹤到根CA證書。

- 如果沒有提供任何中間證書作為輸入。

- 如果缺少伺服器的私鑰，或者無法使用伺服器的私鑰驗證正在上

在將證書上傳到CSM之前，必須聯絡頒發證書的CA來更正這些問題。

在選擇此選項之前，必須使用選項4驗證證書。

僅當沒有中間證書並且只有由突出的根CA證書簽名的伺服器證書時，

如果根CA不是CSM信任的CA，請不要選擇此選項。

在這種情況下，您必須從CA取得用於簽署憑證的根CA憑證，然後使

選擇此選項並提供證書位置時，實用程式：

5 將單個伺服器證書上傳到伺服器

- 驗證憑證是否採用Base64 Encoded X.509憑證格式。

- 顯示證書的主題和頒發證書的詳細資訊。

- 驗證證書在伺服器上是否有效。

- 驗證伺服器私鑰和輸入伺服器證書是否匹配。

- 驗證伺服器證書是否可跟蹤到所需的用於簽名的根CA證書。

驗證成功完成後，應用工具會將證書上傳到CiscoWorks伺服器。

實用程式顯示一個錯誤：

- 如果輸入證書不是所需的格式
- 如果證書日期無效或證書已過期。
- 如果無法驗證伺服器證書，或無法跟蹤到根CA證書。
- 如果缺少伺服器的私鑰，或者無法使用伺服器的私鑰驗證正在上傳的證書，您必須先與頒發證書的CA聯絡以更正這些問題，然後再在CSM中上傳證書。在選擇此選項之前，必須使用選項4驗證證書。

如果要上傳證書鏈，請選擇此選項。如果您也正在上傳根CA憑證，您必須選擇此選項並提供證書位置時，實用程式：

- 驗證憑證是否採用Base64 Encoded X.509憑證格式。
- 顯示證書的主題和頒發證書的詳細資訊。
- 驗證證書在伺服器上是否有效
- 驗證伺服器私鑰和伺服器證書是否匹配。
- 驗證伺服器證書是否可以跟蹤到用於簽名的根CA證書。
- 如果提供了中間鏈，則構建證書鏈並驗證該鏈是否以正確的根CA證書

6 將證書鏈上傳到伺服器


驗證成功完成後，伺服器憑證將上傳到CiscoWorks伺服器。所有中間證書和根CA證書都將上傳並複製到CSM TrustStore。

實用程式顯示一個錯誤：

- 如果輸入證書不是所需的格式。
- 如果證書日期無效或證書已過期。
- 如果無法驗證伺服器證書，或無法跟蹤到根CA證書。
- 如果沒有提供任何中間證書作為輸入。

7 修改公共服務證書

如果缺少伺服器的私鑰，或者無法使用伺服器的私鑰驗證正在上傳的證書，您必須先與頒發證書的CA聯絡以更正這些問題，然後再在CiscoWorks中上傳證書。此選項允許您修改Common Services Certificate中的Host Name條目。如果要更改現有的主機名條目，可以輸入備用主機名。



```
Administrator: Command Prompt

*** SSL Utility ***

Note: Any Certificate given as input to this script should be in Base64-Encoded X.509Certificate format

You have the following options

1. Display Server Certificate Information
2. Display the input Certificate Information
3. Display Root CA Certificates trusted by Server
4. Verify the input Certificate/ Certificate Chain
5. Upload Single Server Certificate to Server
6. Upload a Certificate Chain to Server
7. Modify Common Services Certificate
8. Quit

Enter your choice [1-8]:8
```

步驟2 使用**選項1**取得目前憑證的副本並儲存以備日後參考。

步驟3 開始證書上傳過程之前，請在Windows命令提示符下使用此命令停止CSM守護程式管理器。

```
net stop crmdmgt
```

注意：使用此命令時，CSM服務會關閉。請確保在此過程中沒有任何部署處於活動狀態。

步驟4 再次開啟SSL實用程式。通過導航到前面提到的路徑並使用此命令，可使用命令提示符開啟此實用程式。

```
perl SSLUtil.pl
```

步驟5 選擇選項4。驗證輸入憑證/憑證鏈結。

步驟6 輸入憑證位置 (伺服器憑證和中間憑證)。

注意:指令碼驗證伺服器證書是否有效。驗證完成後，實用程式將顯示選項。如果指令碼在驗證和驗證過程中報告錯誤，則SSL實用程式將顯示用於更正這些錯誤的說明。請按照說明更正這些問題，然後再次嘗試相同選項。

步驟7 選擇接下來的兩個選項中的任意一個。

如果只有一個證書要上傳，即伺服器證書由根CA證書簽名，請選擇**選項5**。

或

如果要上傳的憑證鏈結，也就是如果有伺服器憑證和中間憑證，請選擇**選項6**。

註：如果CSM守護程式管理器尚未停止，CiscoWorks不允許繼續上傳。如果正在上傳的伺服器證書中檢測到主機名不匹配，實用程式將顯示警告消息，但可以繼續上傳。

步驟8 輸入這些所需的詳細資訊。

- 證書的位置
- 中間證書的位置 (如果有)。

如果所有詳細資訊都正確且證書滿足CSM對安全證書的要求，SSL實用程式將上傳證書。

步驟9 重新啟動CSM守護程式管理器以使新的更改生效，並啟用CSM服務。

```
net start crmdmgt
```

註：等待全部CSM服務重新啟動總計為10分鐘。

步驟10 確認CSM正在使用已安裝的身份證書。

註:不要忘記在建立SSL連線至CSM的PC或伺服器上安裝根和中間CA證書。