

CSM -如何安装GUI访问的第三方SSL证书

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[从用户界面的CSR创建](#)

[身份证书加载到CSM服务器里](#)

简介

Cisco Security Manager (CSM)提供一个选项使用第三方证书权限发出的安全证书(CA)。这些证书，当组织策略防止使用CSM自签名证书或要求系统使用从特定CA时，获取的证书可以使用。

TLS/SSL使用这些证书CSM服务器和客户端浏览器之间的通信。本文描述步骤生成一证书签名请求(CSR)在CSM和如何安装标识和根CA证书在同样。

先决条件

要求

Cisco 建议您了解以下主题：

- SSL证书体系结构知识。
- Cisco Security Manager基础知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Security Manager版本4.11和以上。

从用户界面的CSR创建

此部分描述如何生成CSR。

步骤1.运行Cisco Security Manager主页并且选择**服务器管理>Server > Security >单服务器Management>证书设置**。

步骤2.输入为字段要求的值描述在此表里：

字段	使用注释
国家名	双重人格的国家代码。
状态或省	双重人格的状态或省代码或状态或省的完整名称。

现场 双重人格的城市或城镇代码或城市或城镇的完整名称。

单位名称 完成您的组织或简称名称。

组织单位名称 完成您的部门或简称名称。

服务器名称 DNS名，计算机的IP地址或主机名。

电子邮件地址 输入与一个适当和可解决域名的服务器名。这在您的证书显示(是否自己签署的或第三方发出)

电子邮件地址 邮件必须被发送的电子邮件地址。

Certificate Setup

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.

步骤3.单击应用创建CSR。

进程生成以下文件：

- server.key —服务器的专用密钥。
- server.crt —服务器的自签名证书。
- server.pk8 —在PKCS#8格式的服务器的专用密钥。
- server.csr —证书签名请求(CSR)文件。

Note: 这是生成的文件的路径。

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

Note: 如果证书是自签名证书，则您不能修改此信息。

身份证书加载到CSM服务器里

此部分描述如何上传CA提供的身份证书给CSM服务器

Step1发现SSL工具脚本可用在此位置

NMSROOT\MDC\Apache

Note: 必须由CSM安装的目录替换NMSROOT。

此工具有这些选项。

号码 选项

1 显示服务器证书信息

什么它...

- 显示CSM服务器的证书详细信息。

对于第三方已签发证书，此选项显示服务器证书、半成品证书，若有

- 如果证书有效，验证。

此选项接受证书作为输入和：

2 显示输入证书信息

- 验证证书是否在编码的X.509证书格式。
- 显示证书和发出的证书的详细信息主题。
- 验证证书是否是有效在服务器。

3 显示服务器委托的根CA证书

生成所有根CA证书列表。

验证第三方发出的服务器证书CA，是否可以上传。

当您选择此选项，工具：

- 如果证书在Base64编码的X.509Certificate格式，验证。
- 如果证书是有效在服务器，验证
- 如果服务器专用密钥和输入服务器证书配比，验证。
- 验证，如果服务器证书可以跟踪到签字的需要的根CA证书。
- 修建证书链，如果半成品一系列也给，并且验证，如果一系列以

4 验证输入证书或证书链

在验证顺利地完成后，提示您上传证书到CSM服务器。

工具显示错误：

- 如果输入证书不在需要的请格式化
- 如果证书日期无效或，如果证书已经超时。
- 如果服务器证书不可能验证或跟踪到根CA证书。
- 如果其中任一半成品证书未给作为输入。

• 如果服务器的专用密钥未命中或，如果上传的服务器证书不可能您必须与发出证书更正这些问题的CA联系，在您上传证书对CSM前。

在您选择此选项前，您必须验证证书使用选项4。

请选择此选项，只有当没有半成品证书，并且有一个突出的根CA证书

如果根CA不是CSM委托的一个，请勿选择此选项。

在这类情况下，使用选项6.，您必须从CA获取签署证书使用的根CA证书

当您选择此选项，并且提供证书的位置，工具：

5 加载对服务器的单个服务器证书

- 验证证书是否在Base64编码的X.509证书格式。
- 显示证书和发出的证书的详细信息主题。
- 验证证书是否是有效在服务器。
- 验证服务器专用密钥和输入服务器证书是否配比。

• 验证使用签字的服务器证书是否可以跟踪到需要的根CA证书。
在验证顺利地完成后，工具上传证书到CiscoWorks服务器。

工具显示错误：

- 如果输入证书不在需要的请格式化
- 如果证书日期无效或，如果证书已经超时。
- 如果服务器证书不可能验证或跟踪到根CA证书。
- 如果服务器的专用密钥未命中或，如果上传的服务器证书不可能您必须与发出证书更正这些问题的CA联系，在您再前上传在CSM的

在您选择此选项前，您必须验证证书使用选项4。
如果上传证书链，选择此选项。如果也也上传根CA证书，您必须包
当您选择此选项并且提供证书的位置，工具：

- 验证证书是否在Base64编码的X.509证书格式。
 - 显示证书和发出的证书的详细信息主题。
 - 验证证书是否是有效在服务器
 - 验证服务器专用密钥和服务器证书是否配比。
 - 验证使用签字的服务器证书是否可以跟踪到根CA证书。
 - 修建证书链，如果半成品一系列给并且验证，如果一系列以适当在验证顺利地完成后，服务器证书上传到CiscoWorks服务器。
- 所有半成品证书和根CA证书上传并且复制对CSM TrustStore。

6 上传证书链到服务器

工具显示错误：

- 如果输入证书不在需要的请格式化。
 - 如果证书日期无效或，如果证书已经超时。
 - 如果服务器证书不可能验证或跟踪到根CA证书。
 - 如果其中任一半成品证书未给作为输入。
 - 如果服务器的专用密钥未命中或，如果上传的服务器证书不可能您必须与发出证书更正这些问题的CA联系，在您再前上传在CiscoW
- 此选项允许您修改在共同性服务证书的主机名名称条目。
如果希望更改现有主机名名称条目，您能输入一备选主机名。

7 修改共同性服务证书



```
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
```

步骤2请使用选项1获得当前证书的复制和保存它供将来参考。

步骤3终止使用此on命令Windows Prompt命令的CSM守护程序管理器在开始证书加载进程前。

```
net stop crmdmgt
```

Note: CSM服务沿着走使用此命令。在此步骤期间，确保那里是没有部署活跃。

步骤4再次打开SSL工具。此工具可以打开使用Prompt命令被导航对以前被提及的路径和使用此命令。

```
perl SSLUtil.pl
```

步骤5选择**选项4**.验证输入认证证书链。

步骤6输入证书位置(服务器证书和中间证书)。

Note: 如果服务器证书有效，脚本验证。在验证完成后，工具显示选项。如果脚本在验证和验证时报告错误，SSL工具显示指令更正这些错误。遵从说明更正那些问题再次然后尝试同一个选项。

步骤7选择下两个选项中的任一个。

选择**选项5**，如果只有上传的一证书，那是，如果服务器证书由根CA证书签字。

或者

选择**选项6**，如果有上传的证书链，那是，如果有服务器证书和中间证书。

Note: 如果CSM守护程序管理器未被终止，CiscoWorks不准许继续进行加载。工具显示警告消息，如果有在服务器证书检测的主机名不匹配上传，但是加载可以继续。

步骤8输入这些需要的详细信息。

- 证书的位置
- 半成品证书的位置，如果其中任一。

SSL工具上传证书，如果所有详细信息正确，并且证书符合安全证书的CSM要求。

步骤9重新启动新的更改的CSM守护程序管理器能生效和启用CSM服务。

```
net start crmdmgt
```

Note: 为所有的等候CSM服务将被重新启动的10分钟所有。

步骤10确认CSM使用安装的身份证书。

Note: 请勿忘记安装根和半成品CA证书在PC或服务器从SSL连接stablished对CSM。