CSM — 如何安装第三方SSL证书以进行GUI访问

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[从用户界面创建CSR](#)
[身份证书上传到CSM服务器](#)

简介

思科安全管理器(CSM)提供了使用第三方证书颁发机构(CA)颁发的安全证书的选项。当组织策略阻止使用CSM自签名证书或要求系统使用从特定CA获取的证书时，可使用这些证书。

TLS/SSL使用这些证书在CSM服务器和客户端浏览器之间进行通信。本文档介绍在CSM中生成证书签名请求(CSR)的步骤，以及如何在同一位置安装身份和根CA证书。

先决条件

要求

Cisco 建议您了解以下主题：

- SSL证书架构知识。
- 思科安全管理器的基本知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全管理器4.11及更高版本。

从用户界面创建CSR

本节介绍如何生成CSR。

步骤1.运行Cisco Security Manager主页，然后选择**Server Administration > Server > Security > Single-Server Management > Certificate Setup。**

步骤2.输入下表所述字段所需的值：

字段	**使用注释**
国家/地区名称	两个字符的国家/地区代码。
州或省	两个字符的省/自治区代码或省/自治区的完整名称。

地区	两个字符的城市或城镇代码或城市或城镇的完整名称。
单位名称	您的组织的完整名称或缩写。
组织单位名称	部门的完整名称或缩写。
服务器名称	计算机的DNS名称、IP地址或主机名。 输入具有正确且可解析域名的服务器名称。这显示在您的证书上（无论是自签名还是第三方 不应提供本地主机或127.0.0.1。
电子邮件地址	邮件必须发送到的电子邮件地址。

步骤3.单击“**应用**”(Apply)创建CSR。

进程生成以下文件：

- server.key — 服务器的私钥。
- server.crt — 服务器的自签名证书。
- server.pk8 - PKCS#8格式的服务器私钥。
- server.csr — 证书签名请求(CSR)文件。

注意：这是生成文件的路径。
~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

注意：如果证书是自签名证书，则无法修改此信息。

身份证书上传到CSM服务器

本节介绍如何将CA提供的身份证书上传到CSM服务器

第1步查找此位置可用的SSL实用程序脚本

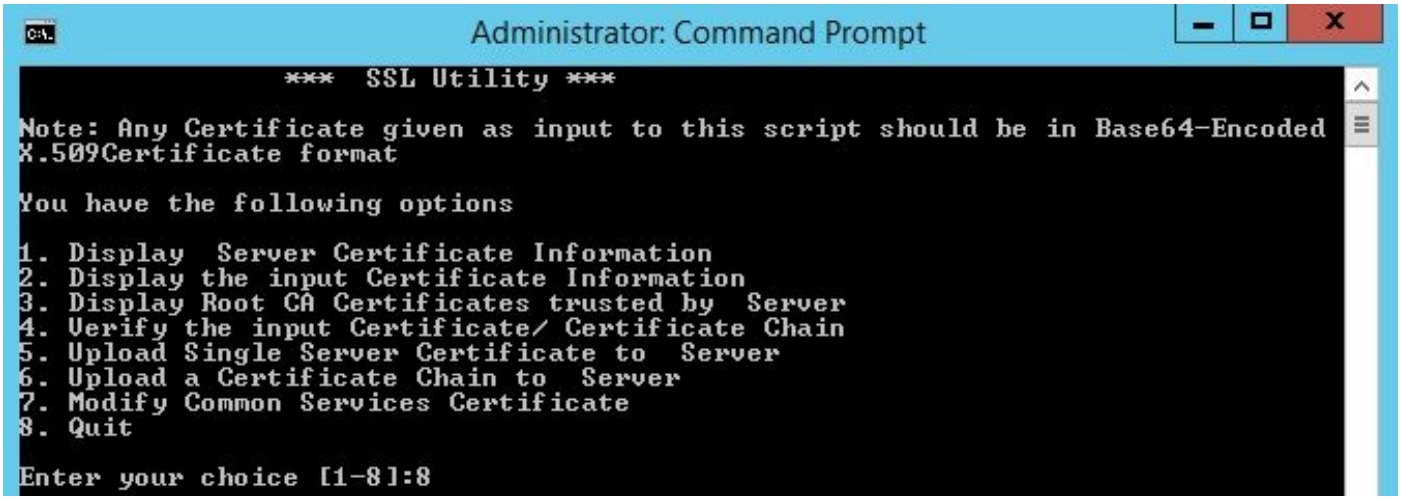
```
NMSROOT\MDC\Apache
```

注意：NMSROOT必须替换为安装CSM的目录。

此实用程序有以下选项。

编号	选项	功能...
1	显示服务器证书信息	• 显示CSM服务器的证书详细信息。 对于第三方颁发的证书，此选项显示服务器证书、中间证书（如果有
2	显示输入的证书信息	• 验证证书是否有效。 此选项接受证书作为输入，并且： • 验证证书是否采用编码的X.509证书格式。 • 显示证书的使用者和颁发证书的详细信息。 • 验证证书在服务器上是否有效。
3	显示服务器信任的根CA证书	生成所有根CA证书的列表。 验证是否可以上传由第三方CA颁发的服务器证书。
4	验证输入证书或证书链	选择此选项时，实用程序： • 验证证书是否采用Base64编码X.509证书格式。 • 验证证书在服务器上是否有效 • 验证服务器私钥和输入服务器证书是否匹配。 • 验证服务器证书是否可以跟踪到所需的根CA证书，使用该证书签 • 构建证书链（如果也提供中间链），并验证链是否以正确的根CA 验证成功完成后，系统将提示您将证书上传到CSM服务器。 实用程序显示错误： • 如果输入证书不是必需格式 • 如果证书日期无效或证书已过期。 • 如果无法验证服务器证书或跟踪到根CA证书。 • 如果任何中间证书未作为输入提供。 • 如果服务器的私钥丢失，或者无法使用服务器的私钥验证正在上 在将证书上传到CSM之前，必须联系颁发证书的CA以更正这些问题。
5	将单个服务器证书上传到服务器	在选择此选项之前，必须使用选项4验证证书。 仅当没有中间证书且只有由突出的根CA证书签名的服务器证书时，才 如果根CA不是CSM信任的CA，请勿选择此选项。 在这种情况下，您必须从CA获取用于签名证书的根CA证书，并使用 选择此选项并提供证书的位置后，实用程序： • 验证证书是否为Base64编码X.509证书格式。 • 显示证书的使用者和颁发证书的详细信息。 • 验证证书在服务器上是否有效。 • 验证服务器私钥和输入服务器证书是否匹配。 • 验证是否可以跟踪服务器证书到用于签名的所需根CA证书。 验证成功完成后，该实用程序将证书上传到CiscoWorks Server。

		实用程序显示错误： • 如果输入证书不是必需格式 • 如果证书日期无效或证书已过期。 • 如果无法验证服务器证书或跟踪到根CA证书。 • 如果服务器的私钥丢失，或者无法使用服务器的私钥验证正在上 在CSM中再次上传证书之前，必须联系颁发证书的CA以更正这些问 在选择此选项之前，必须使用选项4验证证书。
6	将证书链上传到服务器	如果上传证书链，请选择此选项。如果还上传根CA证书，则必须将其 选择此选项并提供证书的位置时，实用程序： • 验证证书是否为Base64编码X.509证书格式。 • 显示证书的使用者和颁发证书的详细信息。 • 验证证书在服务器上是否有效 • 验证服务器私钥与服务器证书是否匹配。 • 验证是否可以跟踪服务器证书到用于签名的根CA证书。 • 构建证书链（如果已提供中间链），并验证链是否以正确的根CA 验证成功完成后，服务器证书将上传到CiscoWorks Server。 所有中间证书和根CA证书都上传并复制到CSM TrustStore。 实用程序显示错误： • 如果输入证书不是必需的格式。 • 如果证书日期无效或证书已过期。 • 如果无法验证服务器证书或跟踪到根CA证书。 • 如果任何中间证书未作为输入提供。 • 如果服务器的私钥丢失，或者无法使用服务器的私钥验证正在上 您必须联系颁发证书的CA以更正这些问题，然后才能再次在CiscoW
7	修改公用服务证书	此选项允许您修改公共服务证书中的主机名条目。 如果要更改现有主机名条目，可以输入备用主机名。



第2步使**用选**项1获取当前证书的副本并保存以备将来参考。

第3步在Windows命令提示符下使用此命令停止CSM后台守护程序管理器，然后开始证书上传过程。

```
net stop crmdmgtd
```

注意:CSM服务使用此命令关闭。确保在此过程中没有活动的部署。

第4步再次打开SSL实用程序。通过导航至前面提到的路径并使用此命令，可以使用命令提示符打开

此实用程序。

```
perl SSLUtil.pl
```

第5步选择**选项4**。验**证输入的证书/证书链**。

第6步输入证书位置（服务器证书和中间证书）。

> **注**意：脚本验证服务器证书是否有效。验证完成后，实用程序将显示这些选项。如果脚本在验证和验证期间报告错误，SSL实用程序将显示纠正这些错误的说明。请按照说明纠正这些问题，然后再试一次相同的选项。

第7步选择接下来两个选项中的任意一个。

如果只有一个证书要上传（即服务器证书由根CA证书签名），请选择**选项5**。

或者

如果有要上传的证书链（即有服务器证书和中间证书），请选择**选项6**。

> 注意：如果CSM守护程序管理器未停止，CiscoWorks不允许继续上载。如果在正在上载的服务器证书中检测到主机名不匹配，实用程序将显示警告消息，但可以继续上载。

第8步输入这些所需的详细信息**。**

- 证书的位置
- 中间证书的位置（如果有）。

如果所有详细信息都正确且证书符合安全证书的CSM要求，SSL实用程序会上传证书。

第9步重新启动CSM守护程序管理器，使新更改生效并启用CSM服务。

```
net start crmdmgtd
```

> **注**意：等待10分钟，以便所有CSM服务重新启动。

第10步确认CSM使用安装的身份证书。

> 注意: **不要忘记在PC或服务器中安装根和中间CA证书，PC或服务器将SSL连接建立到CSM。**