更新Expressway证书

目录

[简介](#)
[背景信息](#)
[Process](#)
[A)从当前证书获取信息](#)
[B)生成CSR（证书签名请求）并将其发送到CA（证书颁发机构）进行签名。](#)
[C)检查新证书中的SAN列表和扩展/增强型密钥使用属性](#)
[D)检查签署新证书的CA与签署旧证书的CA是否相同](#)
[E)安装新证书](#)

简介

本文档介绍Expressway/视频通信服务器(VCS)证书续订流程。

本文档中的信息适用于Expressway和VCS。文档引用了Expressway，但可以与VCS互换。

> **注意：**虽然本文档旨在帮助您完成证书续订流程，但最好还要检查适用于您的版本的Cisco Expressway证书创建和使用部署指南。

背景信息

无论何时更新证书，都必须考虑两个要点，以确保系统在安装新证书后继续正常运行：

1.新证书的属性必须与旧证书的属性匹配（主要是使用者替代名称和扩展密钥用法）

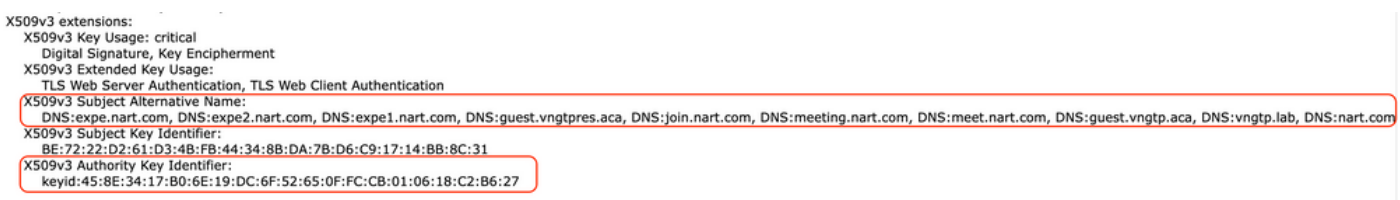
2.用于签署新证书的CA（证书颁发机构）必须受与Expressway直接通信的其他服务器（例如CUCM、Expressway-C、Expressway-E等）信任

Process

A)从当前证书获取信息

1.打开Expressway网页维**护>安全>服务器证书> Show decoded。**

2.在打开的新窗口中，将“Subject Alternative name”和“Authority Key Identifier” X509v3扩展名复制到记事本文档。

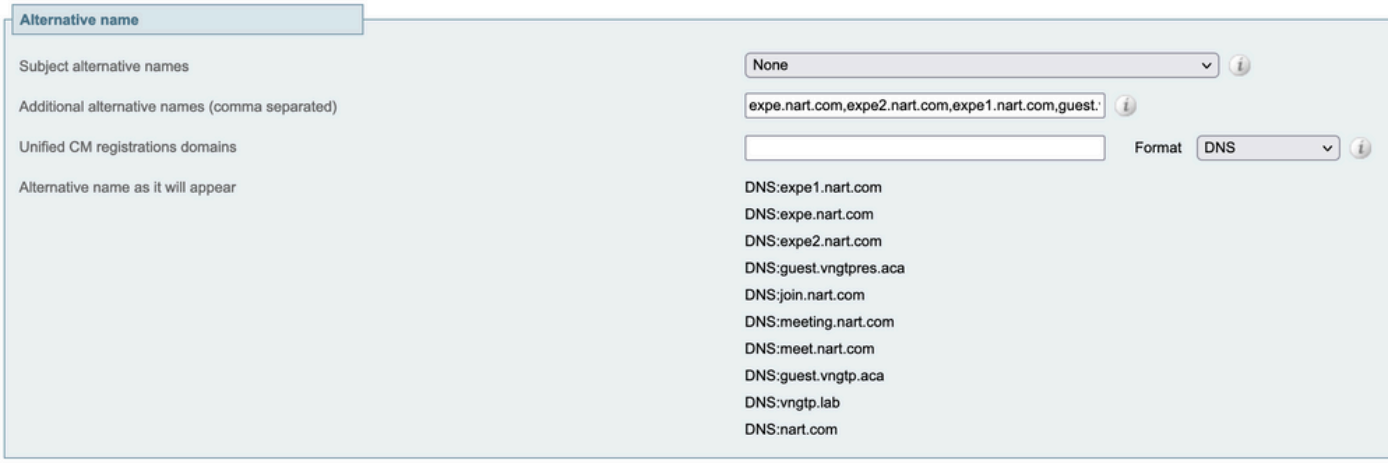


“Show decoded”证书窗口

B)生成CSR（证书签名请求）并将其发送到CA（证书颁发机构）进行签名。

1.从Expressway网页维**护>安全>服务器证书>生成CSR。**

2.在“生成CSR”窗口中，在**Additional alternative names（以逗号分隔）字段**中，填写我们在A部分保存的“主题备用名称”的所有值，并确保删除“DNS：”并将列表以逗号分隔，请参阅图（在“备用名称将显示”旁边，您可以看到证书中要使用的所有SAN的列表）：



生成CSR SAN条目

3.填写**Additional Information**（其他信息）部分下的其余信息，如国家/地区、公司、州/省等，然后单击**Generate CSR**（生成CSR）。

4.生成CSR后，页面**Maintenance > Security > Server Certificate**显示**Discard CSR**和**Download**选项，您必须选择**Download**并将CSR发送到CA进行签名。

> **注意：**确保在安装新证书之前不使用**Discard CSR**，如果已完成**Discard CSR**，然后尝试安装使用已放弃的CSR签名的证书，则证书安装失败。

C)检查新证书中的SAN列表和扩展/增强型密钥使用属性

在Windows证书管理器中打开新签名的证书并检查：

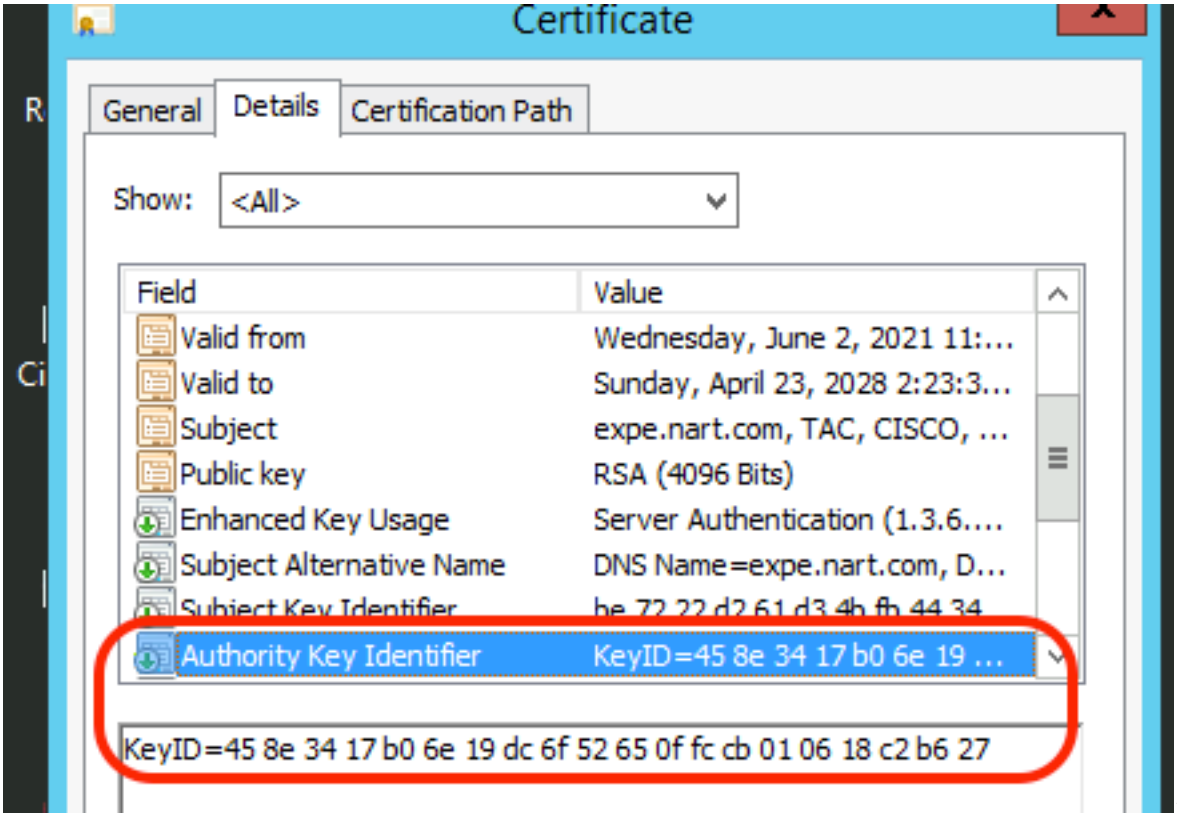
1. SAN列表与我们在生成CSR时使用的A部分中保存的SAN列表匹配。

2. “扩展/增强型密钥用法”属性必须包括“客户端身份验证”和“服务器身份验证”。

> **注意：**如果证书具有.pem扩展名，请将其重命名为.cer或.crt，以便能够使用Windows证书管理器打开它。使用Windows证书管理器打开证书后，您可以转到**Details**选项卡**> Copy to File**并将其导出为Base64编码文件，在文本编辑器中打开时，一个base64编码文件通常顶部有“-----BEGIN CERTIFICATE-----”，底部有“-----END CERTIFICATE-----”

D)检查签署新证书的CA与签署旧证书的CA是否相同

在Windows证书管理器中打开新签名的证书，复制“授权密钥标识符”值，并将其与我们在A部分保存的“授权密钥标识符”值进行比较。



使用Windows证书管理器打开的新证书

如果两个值相同，则意味着使用与旧证书相同的CA来签署新证书，您可以进入E部分来上传新证书。

如果这些值不同，则意味着用于签署新证书的CA不同于用于签署旧证书的CA，并且您必须执行以下步骤才能继续执行E部分：

1.获取所有中间CA证书（如果有）和根CA证书。

2.转到**维护>安全>受信任CA证书**，单击**浏览**，然后在计算机上搜索中间CA证书并上传。对任何其他中间CA证书和根CA证书执行相同操作。

3.对连接到此服务器的任何Expressway E（如果要续订的证书是Expressway C证书）或连接到此服务器的任何Expressway C（如果要续订的证书是Expressway E证书）执行相同的操作。

4.如果要续订的证书是Expressway-C证书，并且您具有MRA或对CUCM具有安全区域，则必须确保CUCM信任新的根和中间CA，并将根和中间CA证书上传到CUCM tomcat-trust和callmanager-trust存储，然后重新启动CUCM上的相关服务。

E)安装新证书

检查完之前的所有点后，您现在可以在Expressway上通过**维护>安全>服务器证书**单击**浏览**，然后从计算机中选择新证书文件并上传它。

安装新证书后，必须重新启动Expressway。

> **注意：**确保从**维护>安全>服务器证书**上传到Expressway的证书只包含Expressway服务器证书，而不包含完整证书链，并确保其Base64证书

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。