

# 使用当前证书中的信息生成新的Expressway证书。

。

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[步骤1.找到当前证书信息。](#)

[步骤2.使用上述信息创建新的CSR。](#)

[步骤3.检验并下载新CSR。](#)

[步骤4.检验新证书中包含的信息。](#)

[步骤5.将新CA证书上传到服务器受信任存储 \( 如果适用 \) 。](#)

[步骤6.将新证书上传到Expressway服务器。](#)

[验证](#)

[故障排除](#)

## 简介

本文档介绍如何使用现有Expressway证书中的信息生成新的证书签名请求(CSR)。

## 先决条件

### 要求

思科建议您了解以下主题：

- 证书属性
- Expressway或视频通信服务器(VCS)

### 使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始 ( 默认 ) 配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 配置

**步骤1.找到当前证书信息。**

要获取当前证书中包含的信息，请导航至Expressway图形用户界面(GUI)上的**维护>安全>服务器证书**(Maintenance > Security > Server Certificate)。

找到“服务器证书数据”部分并选择“显示 ( 解码 )”。

在公用名(CN)和主题备用名(SAN)中查找信息，如图所示：

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      35:00:00:00:a1:4b:f0:c2:00:f6:dd:70:05:00:00:00:00:00:a1
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: DC=local, DC=anmiron, CN=anmiron-SRV-AD-CA
    Validity
      Not Before: Dec  2 04:39:57 2019 GMT
      Not After  : Nov 28 00:32:43 2020 GMT
    Subject: C=MX, ST=CDMX, L=CDMX, O=TAC, OU=TAC, CN=expe.domain.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (4096 bit)
      Modulus:
        -----
X509v3 extensions:
  X509v3 Key Usage: critical
    Digital Signature, Key Encipherment
  X509v3 Extended Key Usage:
    TLS Web Client Authentication, TLS Web Server Authentication
  X509v3 Subject Alternative Name:
    DNS:expe.domain.com, DNS:domain.com
  X509v3 Subject Key Identifier:
    92:D0:D7:24:4A:BC:E3:C0:02:E5:7E:09:5D:78:FF:56:7A:6E:37:5B
  X509v3 Authority Key Identifier:
    keyid:6C:71:80:4C:9A:21:79:DB:C2:7E:23:7A:DB:9B:73:11:E4:35:61:32
```

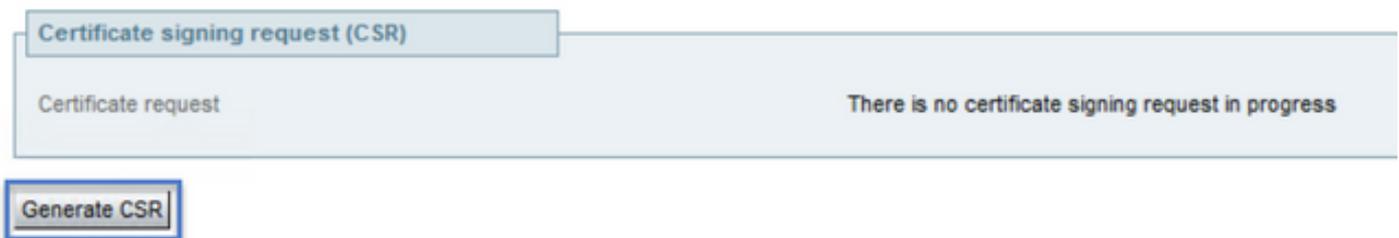
现在，您知道CN和SAN的副本，以便它们可以添加到新的CSR中。

( 可选 ) 您可以复制证书的附加信息，这些信息包括国家(C)、州(ST)、地点(L)、组织(O)、组织单位(OU)。此信息位于CN旁。

## 步骤2.使用上述信息创建新的CSR。

要创建CSR，请导航至“维护”>“安全”>“服务器证书”。

找到“证书签名请求(CSR)”一节，并选择“生成CSR”，如图所示：



输入从当前证书收集的值。

除非CN是集群，否则无法修改它。对于集群，可以选择CN作为Expressway完全限定域名 (FQDN)或集群FQDN。在本文档中，使用一台服务器，因此CN对应于您从当前证书获得的内容，如图所示：

The screenshot shows the 'Generate CSR' section of a web interface. It features a 'Common name' input field with the value 'expe.domain.com'. To the right, there is a label 'FQDN of Expressway'. Below the input field, there is a label 'Common name as it will appear'.

对于SAN，如果它们未自动填充，则必须手动输入这些值，为此，您可以在“其他备用名称”上输入这些值，如果有多个SAN，则它们必须用逗号分隔，例如：example1.domain.com、example2.domain.com、example3.domain.com。添加后，SAN将在“备用名称”部分列出，如图所示：

The screenshot shows the 'Alternative name' section. The 'Additional alternative names (comma separated)' field contains 'domain.com'. Below it, there is a 'Unified CM registrations domains' field and a 'Format' dropdown menu set to 'DNS'. The 'Alternative name as it will appear' field shows 'DNS:domain.com'.

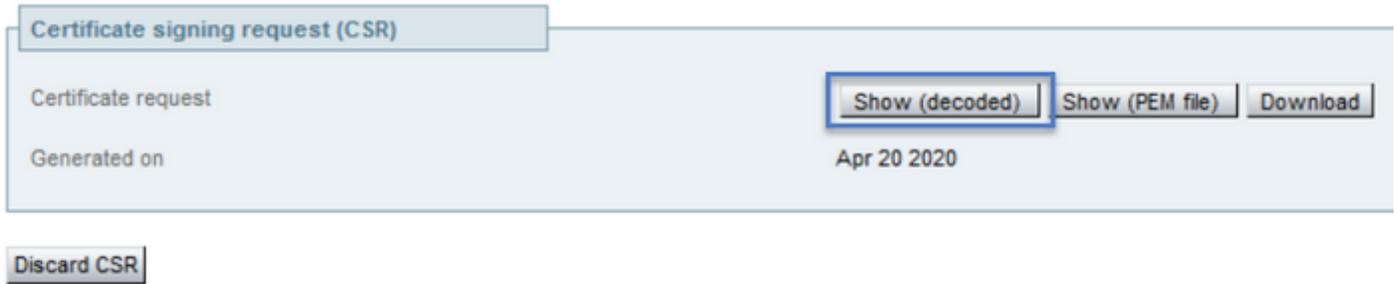
如果未自动填充或必须更改，则需要输入其他信息，如图所示：

The screenshot shows the 'Additional information' section. It contains several fields: 'Key length (in bits)' set to 4096, 'Digest algorithm' set to SHA-256, 'Country' set to MX, 'State or province' set to CDMX, 'Locality (town name)' set to CDMX, 'Organization (company name)' set to TAC, 'Organizational unit' set to TAC, and an empty 'Email address' field. Each field has an information icon (i) to its right. At the bottom left, there is a 'Generate CSR' button.

完成后，选择“生成CSR”。

### 步骤3.检验并下载新CSR。

生成CSR后，您可以在证书签名请求(CSR)部分选择Show(decoded)，以验证所有SAN是否都存在，如图所示：



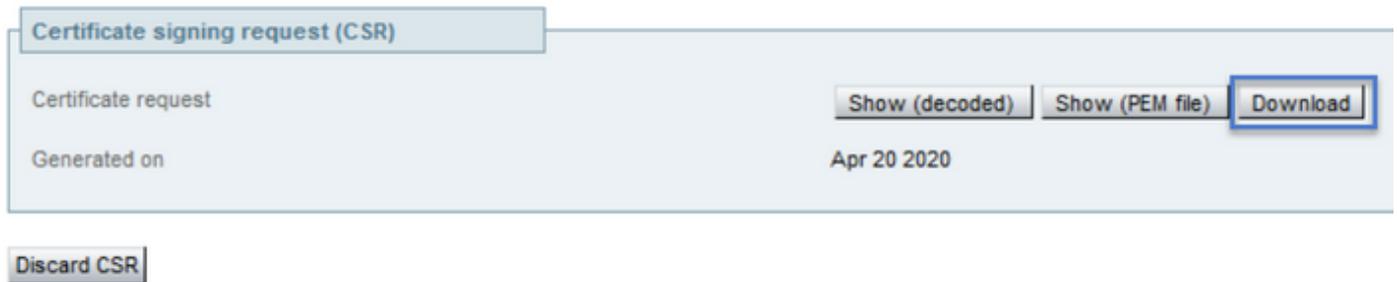
在新窗口中查找CN和主题备用名称，如图所示：

```
Certificate Request:
  Data:
    Version: 0 (0x0)
    Subject: OU=TAC, O=TAC, CN=expe.domain.com, ST=CDMX, C=MX, L=CDMX
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (4096 bit)
      Modulus:
```

CN始终自动添加为SAN:

```
      X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
      X509v3 Subject Alternative Name:
        DNS:expe.domain.com, DNS:domain.com
    Signature Algorithm: sha256WithRSAEncryption
```

现在CSR已验证，您可以关闭新窗口，并在“证书签名请求(CSR)”部分选择“下载(解码)”，如图所示：

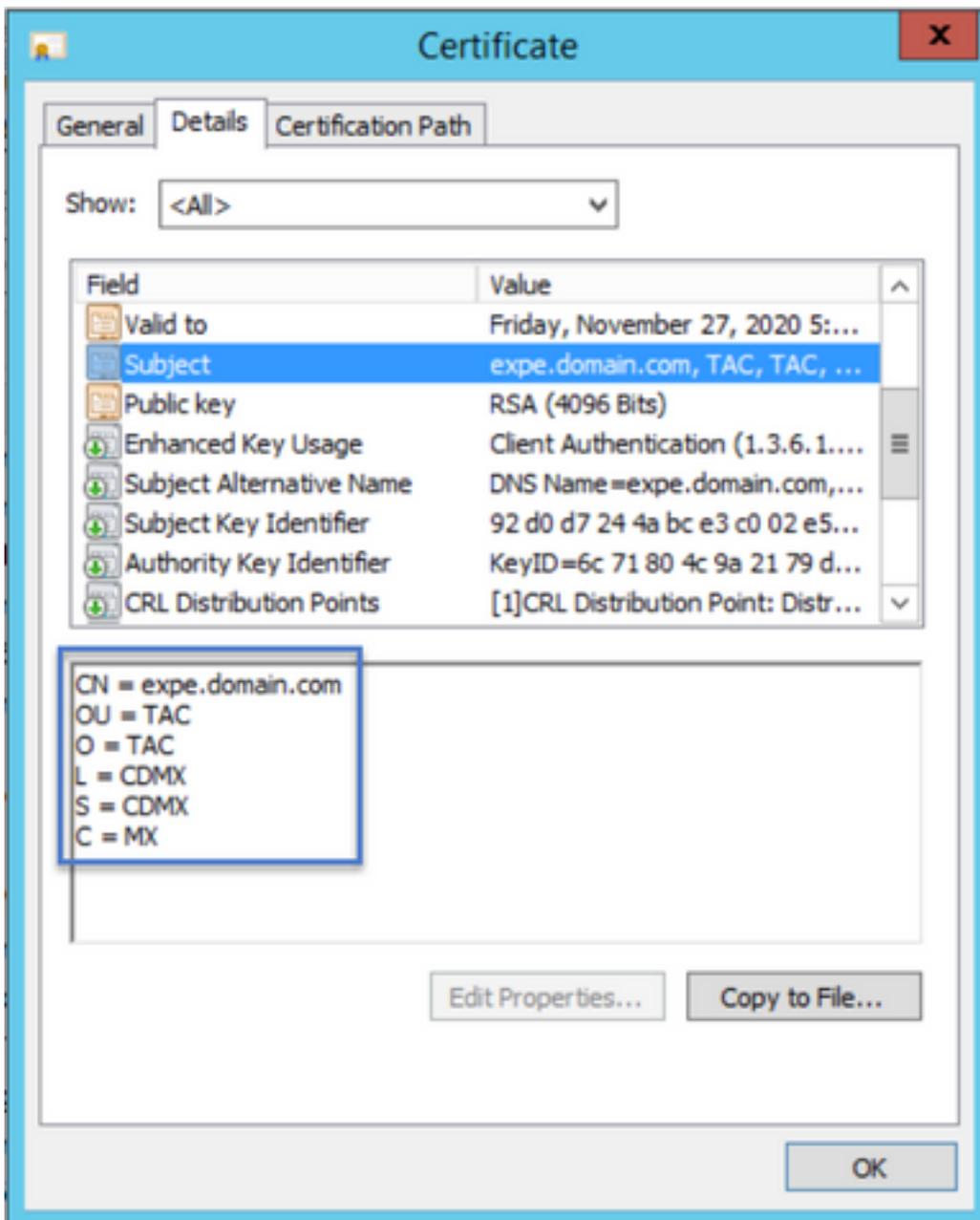


下载后，您可以将新CSR发送到要签名的证书颁发机构(CA)。

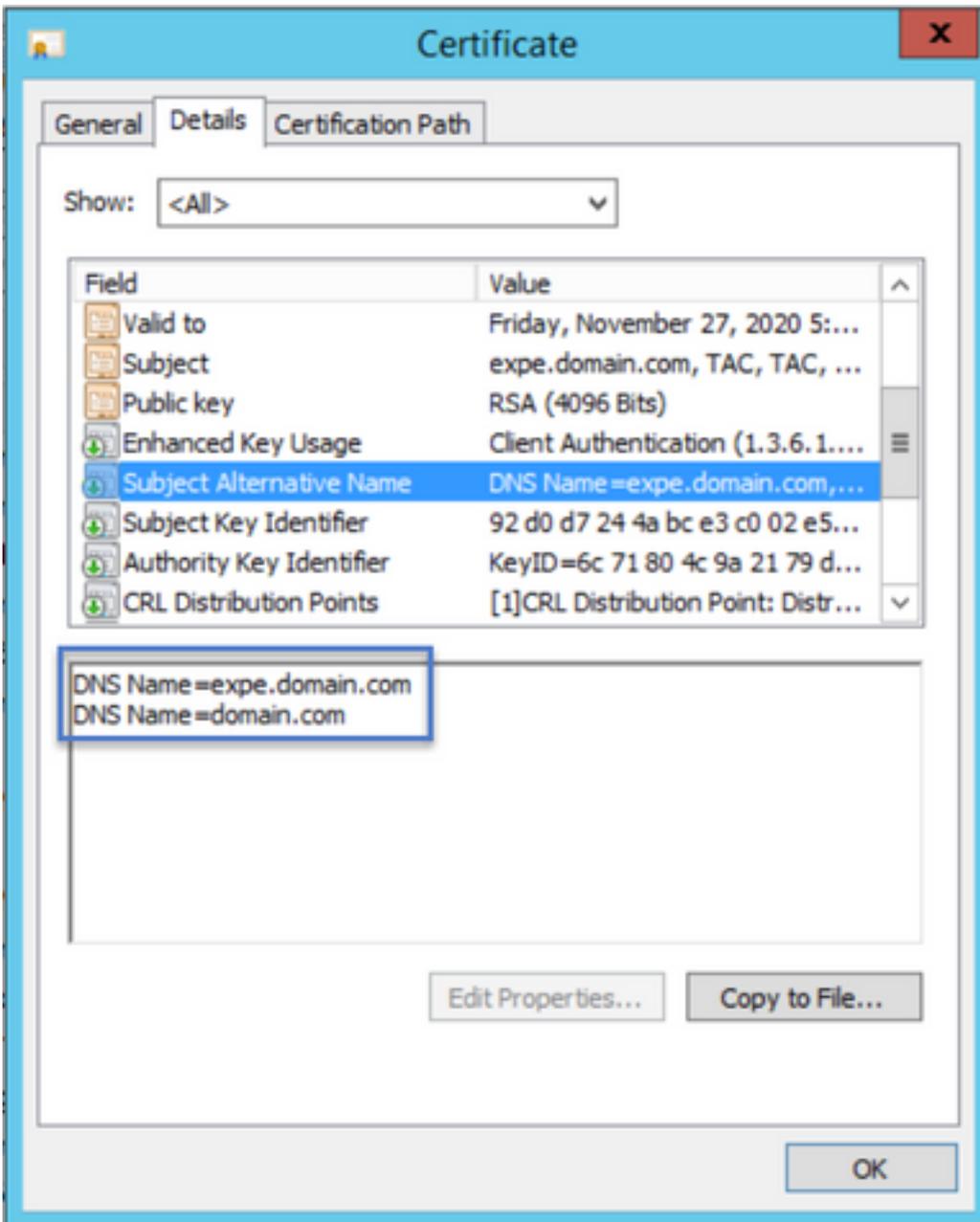
#### 步骤4. 检验新证书中包含的信息。

从CA返回新证书后，您可以验证证书中是否存在所有SAN。为此，您可以打开证书并查找SAN属性。在本文档中，Windows PC用于查看属性，但只要您能打开或解码证书以查看属性，这并非唯一的方法。

打开证书并导航至Details选项卡并查找Subject，它应包含CN和Additional Information，如图所示：



另请查找主题备用名部分，它必须包含您在CSR中输入的SAN，如图所示：



如果您在CSR中输入的所有SAN都不在新证书中，请联系您的CA，查看是否为您的证书允许额外的SAN。

### 步骤5.将新CA证书上传到服务器受信任存储（如果适用）。

如果CA与已签署旧Expressway证书的CA相同，您可以放弃此步骤。如果它是不同的CA，则您必须将新CA证书上传到每个Expressway服务器中的受信任CA列表。如果您在Expressway之间（例如Expressway-C和Expressway-E之间）有传输层安全(TLS)区域，则必须在两台服务器上上传新CA，以便它们能够相互信任。

为此，您可以逐个上传CA证书。导航至Expressway上的**维护>安全>受信任CA证书**。

1. 选择“浏览”。
2. 在新页面上选择CA证书。
3. 选择**添加 CA 证书**。

必须对证书链（根和中间）中的每个CA证书执行此过程，并且必须在所有Expressway服务器中执行，即使这些服务器是集群服务器。

## 步骤6.将新证书上传到Expressway服务器。

如果新证书中的所有信息都正确，请导航至：**维护>安全>服务器证书**。

找到“上传新证书”部分，如图所示：

1. 在“选择服务器证书文件”部分选择“浏览”。
2. 选择新证书。
3. 选择上传服务器证书数据。

Upload new certificate

Select the server private key file

Select the server certificate file

System will use the private key file generated at the same time as the CSR.

Browse... ExpECertNew.cer

Upload server certificate data

如果Expressway接受新证书，Expressway会提示重新启动以应用更改，并且消息显示证书的新过期日期，如图所示：

### Server certificate

Files uploaded: Server certificate updated, however a restart is required for this to take effect.

Certificate info: This certificate expires on Nov 28 2020.

Server certificate data	
Server certificate	Show (decoded) Show (PEM file)
Currently loaded certificate expires on	Nov 28 2020
Certificate Issuer	anmiron-SRV-AD-CA

Reset to default server certificate

要重新启动Expressway，请选择restat。

## 验证

服务器恢复后，必须安装新证书，您可以导航至：**Maintenance > Security > Server Certificate**以便确认。

找到**服务器证书**数据并查找**当前加载的证书**过期日期部分，它显示证书的新过期日期，如图所示：

## Server certificate

### Server certificate data

Server certificate

Show (decoded)

Show (PEM file)

Currently loaded certificate expires on

Nov 28 2020

Certificate Issuer

anmiron-SRV-AD-CA

Reset to default server certificate

## 故障排除

目前没有针对此配置故障排除信息。