

[Generate New Expressway Certificate with the Information from the Current Certificate]

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ステップ1：現在の証明書情報を見つけます。](#)

[ステップ2：上記の情報を使用して新しいCSRを作成します。](#)

[ステップ3：新しいCSRの確認とダウンロード](#)

[ステップ4：新しい証明書に含まれる情報を確認します。](#)

[ステップ5：必要に応じて、新しいCA証明書をサーバの信頼ストアにアップロードします。](#)

[ステップ6：新しい証明書をExpresswayサーバにアップロードします。](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、既存のExpressway証明書の情報を使用して、新しい証明書署名要求 (CSR) を生成する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 証明書の属性
- ExpresswayまたはVideo Communication Server(VCS)

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ステップ1：現在の証明書情報を見つけます。

現在の証明書に含まれている情報を取得するには、Expressway Graphical User Interface(GUI)で Maintenance > Security > Server Certificateに移動します。

[サーバ証明書データ]セクションを見つけ、[表示 (デコード)]を選択します。

図に示すように、共通名(CN)とサブジェクト代替名(SAN)の情報を探します。

```
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
```

これで、CNとSANのコピーが分かり、新しいCSRに追加できるようになります。

必要に応じて、国(C)、州(ST)、地域(L)、組織(O)、組織単位(OU)などの証明書の追加情報をコピーできます。この情報はCNの横にあります。

ステップ2：上記の情報を使用して新しいCSRを作成します。

CSRを作成するには、[Maintenance] > [Security] > [Server Certificate]に移動します。

[証明書の署名要求(CSR)]セクションを探し、図に示す[CSRの生成]を選択します。

Certificate signing request (CSR)

Certificate request There is no certificate signing request in progress

Generate CSR

現在の証明書から収集された値を入力します。

CNは、クラスタでない限り変更できません。クラスタの場合、CNをExpressway完全修飾ドメイン名(FQDN)またはクラスタFQDNとして選択できます。このドキュメントでは、単一のサーバを使用するため、図に示すように、現在の証明書から取得した内容に対応するCNが使用されます。

Generate CSR

Common name

Common name FQDN of Expressway

Common name as it will appear expe.domain.com

SANの場合は、自動入力されていない場合は値を手動で入力する必要があります。これを行うには、複数のSANを使用している場合は、カンマで区切って別の[Additional alternative names]に値を入力します。example1.domain.com、example2.domain.com、example3.domain.com SANを追加すると、図に示すように、[Alternative name]セクションにSANが表示されます。

Alternative name

Additional alternative names (comma separated) ⓘ

Unified CM registrations domains Format DNS ⓘ

Alternative name as it will appear DNS:domain.com

追加情報は必要です。自動入力されていない場合、または変更する必要がある場合は、図に示すように手動で入力する必要があります。

Additional information

Key length (in bits) 4096 ⓘ

Digest algorithm SHA-256 ⓘ

Country ★ MX ⓘ

State or province ★ CDMX ⓘ

Locality (town name) ★ CDMX ⓘ

Organization (company name) ★ TAC ⓘ

Organizational unit ★ TAC ⓘ

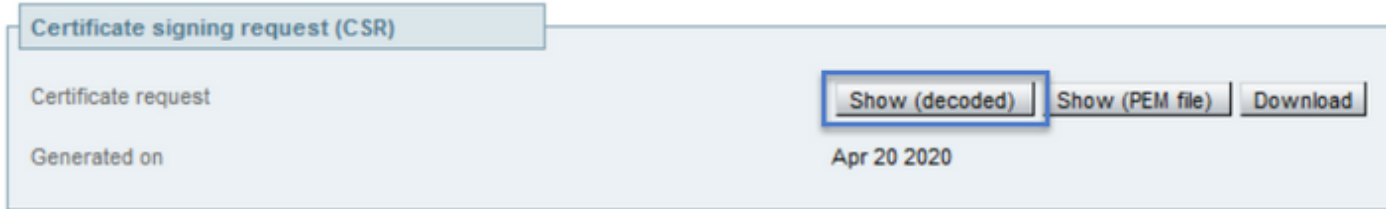
Email address ⓘ

Generate CSR

完了したら、[Generate CSR]を選択します。

ステップ3：新しいCSRの確認とダウンロード

CSRが生成されたら、CSR (証明書署名要求) セクションでShow(decoded)を選択して、図に示すように、すべてのSANが存在することを確認できます。



Discard CSR

図に示すように、新しいウィンドウでCNとSubject Alternative Nameを探します。

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は常にSANとして自動的に追加されます。

X509v3 Extended Key Usage:

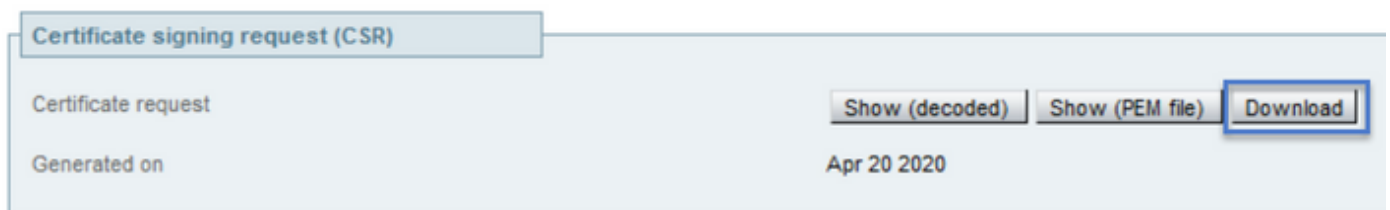
TLS Web Server Authentication, TLS Web Client Authentication

X509v3 Subject Alternative Name:

DNS:expe.domain.com, DNS:domain.com

Signature Algorithm: sha256WithRSAEncryption

CSRが確認できたら、新しいウィンドウを閉じ、図に示すように[Certificate signing request (CSR)]セクションで[Download (decoded)]を選択します。



Discard CSR

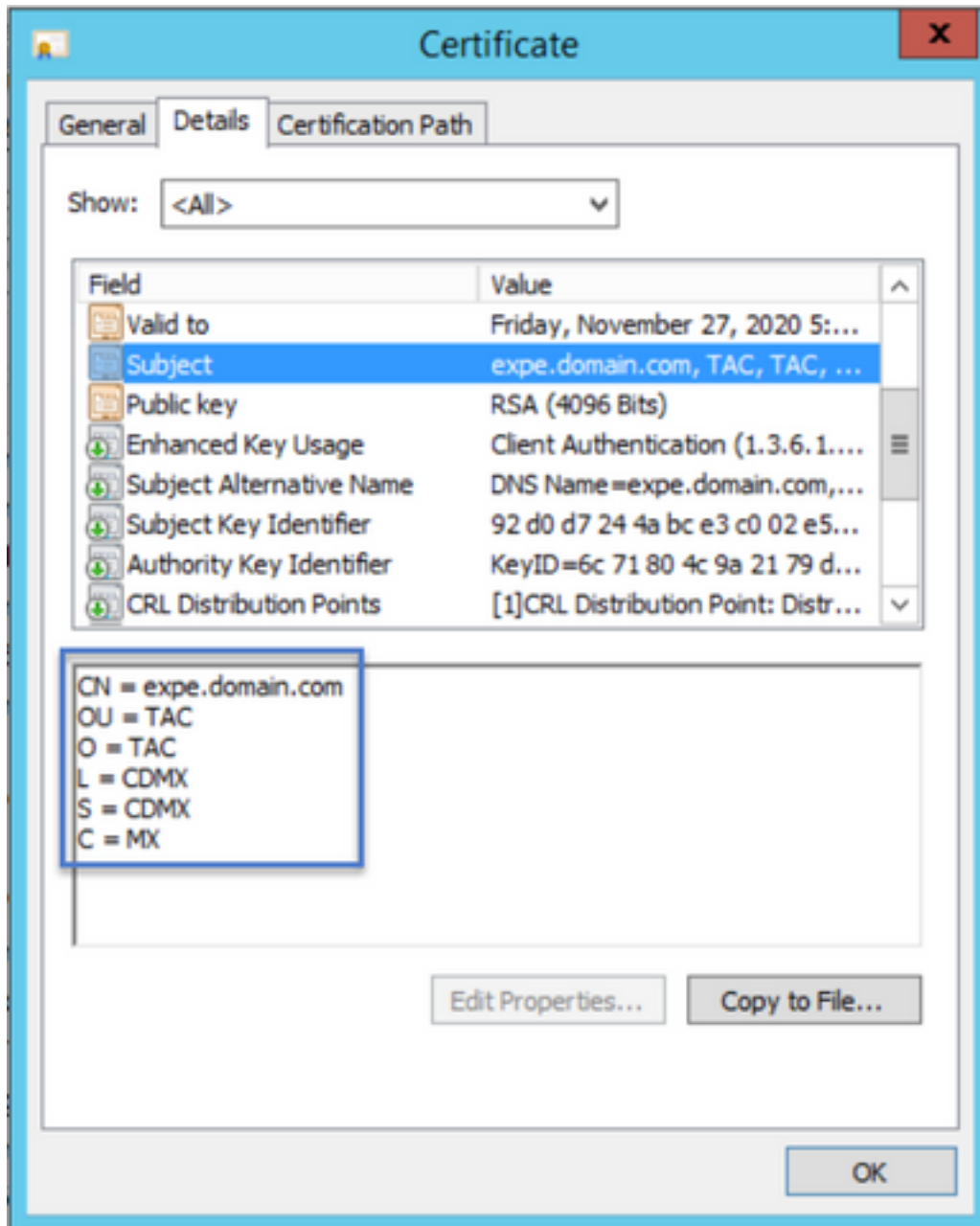
ダウンロード後、新しいCSRを認証局(CA)に送信して署名することができます。

ステップ4：新しい証明書に含まれる情報を確認します。

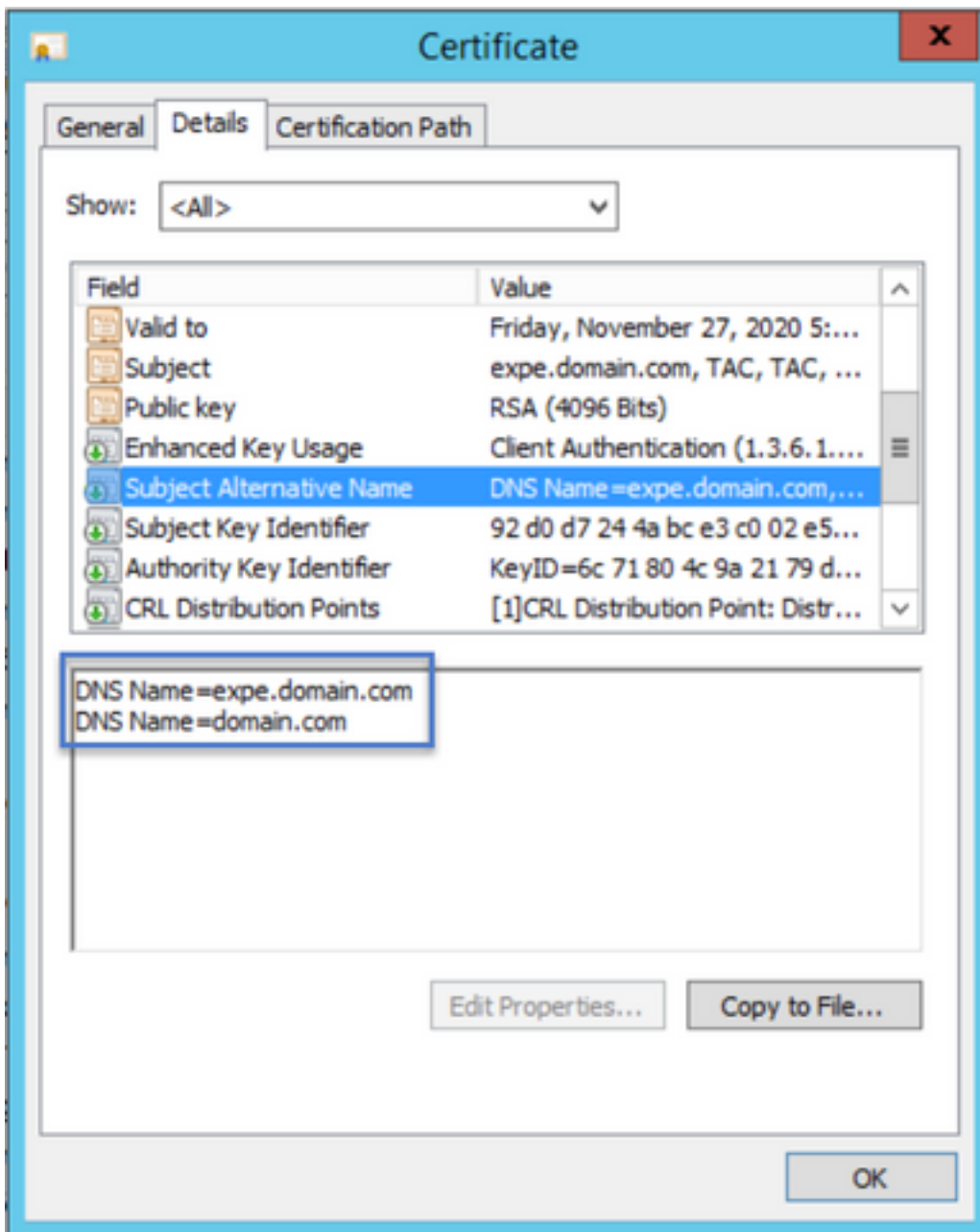
新しい証明書がCAから返されたら、すべてのSANが証明書に存在するかどうかを確認できます。そのためには、証明書を開き、SAN属性を探します。このドキュメントでは、Windows PCを使

用して属性を表示します。証明書を開いたりデコードしたりして属性を確認できる限り、これは唯一の方法ではありません。

証明書を開き、[Details]タブに移動し、[Subject]を探します。図に示すように、CNと追加情報が含まれている必要があります。



[Subject Alternative Name]セクションを探します。図に示すように、CSRに入力したSANが含まれている必要があります。



CSRに入力したすべてのSANが新しい証明書に存在しない場合は、CAに連絡して、証明書に対して追加のSANが許可されているかどうかを確認してください。

ステップ5：必要に応じて、新しいCA証明書をサーバの信頼ストアにアップロードします。

CAが古いExpressway証明書に署名したものと同一場合は、この手順を破棄できます。別のCAである場合は、新しいCA証明書を各Expresswayサーバの信頼できるCAリストにアップロードする必要があります。Expressway-CとExpressway-Eの間など、Expressway間にTransport Layer Security(TLS)ゾーンがある場合は、新しいCAを両方のサーバにアップロードして、相互に信頼できるようにする必要があります。

そのためには、CA証明書を1つずつアップロードします。Expresswayで[Maintenance] > [Security] > [Trusted CA certificates]に移動します。

1. 「参照」を選択します。
2. 新しいページ[Select the CA Certificate]を開きます。
3. [CA 証明書の追加 (Append CA certificate)] を選択します。

この手順は、証明書チェーン（ルートおよび中間証明書）内の各CA証明書に対して実行する必要があり、クラスタ化されている場合でも、すべてのExpresswayサーバで実行する必要があります。

ステップ6：新しい証明書をExpresswayサーバにアップロードします。

新しい証明書のすべての情報が正しい場合、新しい証明書をアップロードするには、次の場所に移動します。[Maintenance] > [Security] > [Server Certificate]を選択します。

図に示すように[Upload new certificate]セクションを探します。

1. [サーバ証明書ファイルの選択]セクションで[参照]を選択します。
2. 新しい証明書を選択します。
3. [サーバ証明書データのアップロード (Upload server certificate data)] を選択します。

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

新しい証明書がExpresswayによって受け入れられた場合、Expresswayは変更を適用するための再起動を求めるプロンプトを表示し、図に示すように、証明書の新しい有効期限が表示されます。

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

Expresswayを再起動するには、[restart]を選択します。

確認

サーバが戻ったら、新しい証明書がインストールされている必要があります。次の場所に移動できます。[Maintenance] > [Security] > [Server Certificate]を選択して確認します。

サーバ証明書データを見つけて、[Currently loaded certificate expires on]セクションを探します。

図に示すように、証明書の新しい有効期限が表示されます。

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

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。