Générez un nouveau certificat Expressway avec les informations du certificat actuel.

Contenu

Introduction

Ce document décrit comment générer une nouvelle demande de signature de certificat (CSR) avec les informations du certificat Expressway existant.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître les sujets suivants :

- Attributs de certificat
- Expressways ou Video Communication Server (VCS)

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

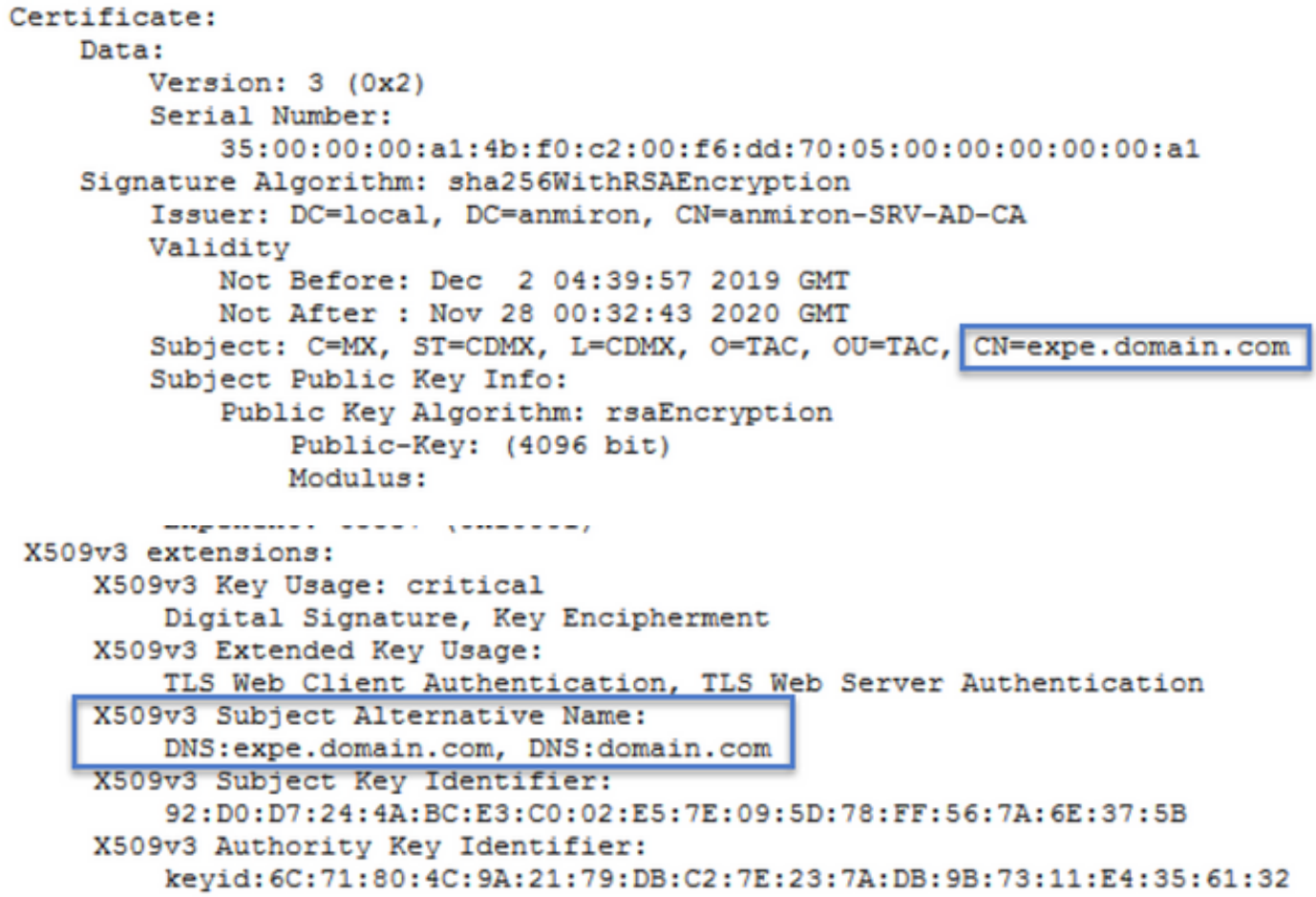
Configuration

Étape 1. Recherchez les informations de certificat actuelles.

Afin d'obtenir les informations contenues dans le certificat actuel, accédez à **Maintenance > Security > Server Certificate** sur l'interface graphique utilisateur d'Expressway.

Recherchez les **données de certificat du serveur** et sélectionnez **Afficher (décodé)**.

Recherchez les informations dans le **nom commun (CN)** et le **SAN (Subject Alternative Name)** comme indiqué sur l'image :



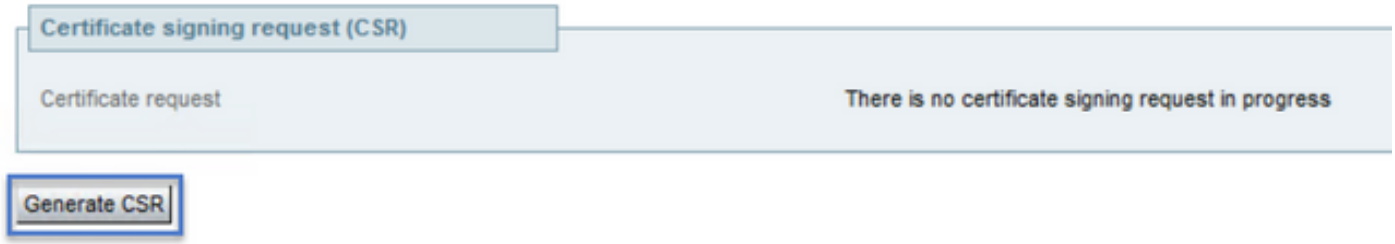
Maintenant que vous connaissez le CN et le SAN, copiez-les afin qu'ils puissent être ajoutés au nouveau CSR.

Vous pouvez éventuellement copier les informations supplémentaires pour le certificat qui est le pays (C), l'État (ST), la localité (L), l'organisation (O), l'unité d'organisation (OU). Ces renseignements sont fournis à côté du CN.

Étape 2. Créez une nouvelle demande de service de contact avec les informations obtenues ci-dessus.

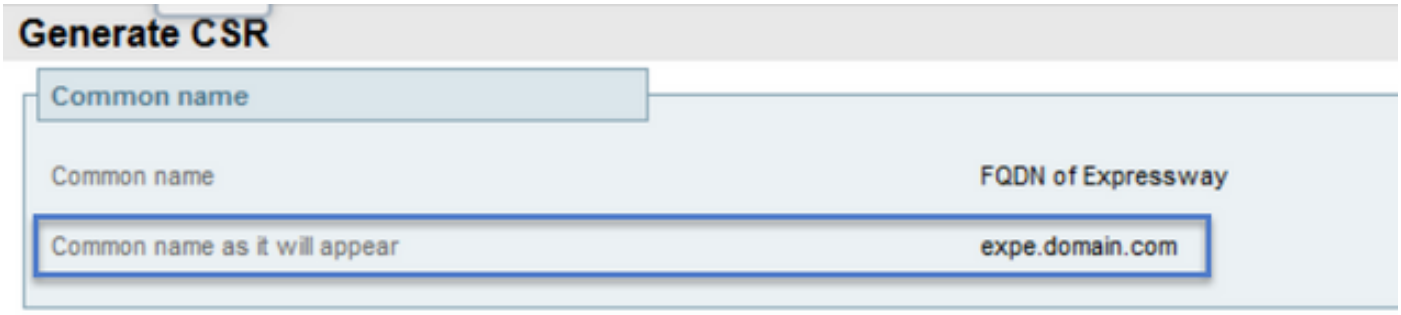
Pour créer le CSR, accédez à **Maintenance > Security > Server Certificate**.

Recherchez la section **Demande de signature de certificat (CSR)** et sélectionnez **Générer CSR** comme indiqué dans l'image :

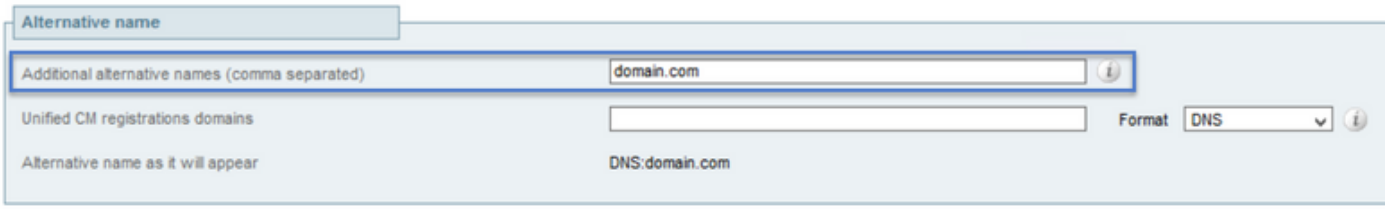


Entrez les valeurs collectées à partir du certificat actuel.

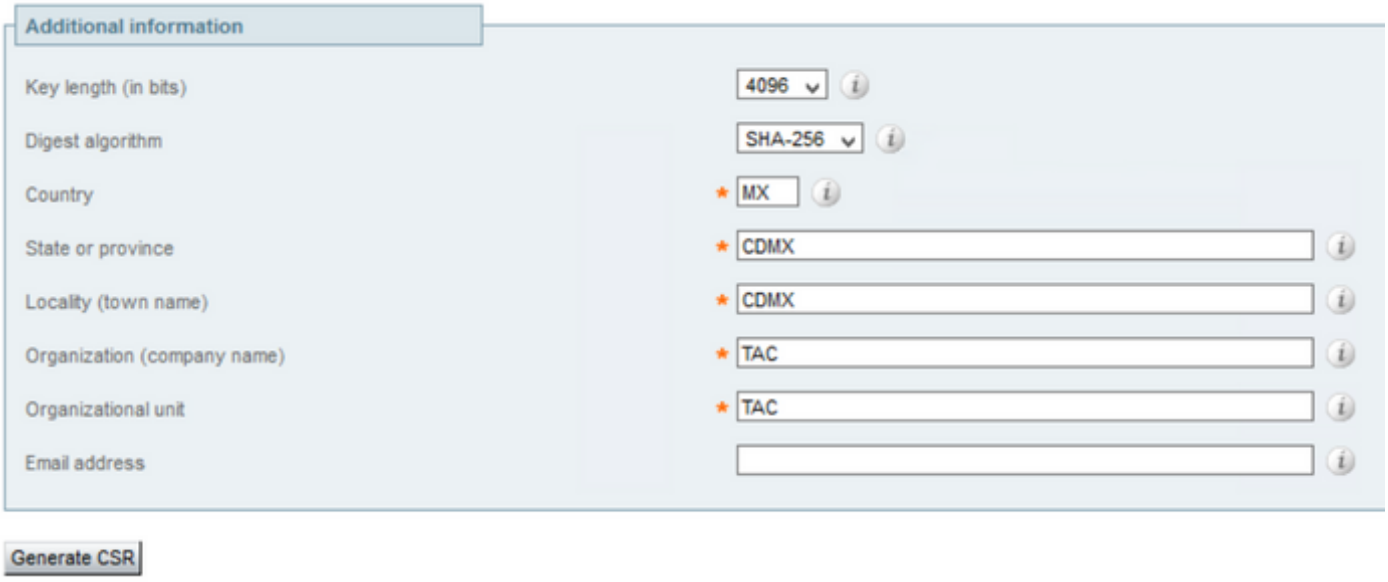
Le CN ne peut être modifié que s'il s'agit d'une grappe. Dans le cas d'un cluster, vous pouvez sélectionner le CN comme nom de domaine complet d'Expressway ou nom de domaine complet du cluster. Dans ce document, un seul serveur est utilisé et le CN correspond donc à ce que vous avez obtenu du certificat actuel, comme l'illustre l'image :



Pour les SAN, vous devez entrer les valeurs manuellement en cas de non-autopulation. Pour ce faire, vous pouvez entrer les valeurs sur les **noms alternatifs supplémentaires**, si vous avez plusieurs SAN, ils doivent être séparés par des virgules par exemple : exemple1.domaine.com, exemple2.domaine.com, exemple3.domaine.com. Une fois ajoutés, les SAN sont répertoriés sur le **nom alternatif tel qu'il apparaîtra** dans la section, comme illustré dans l'image :



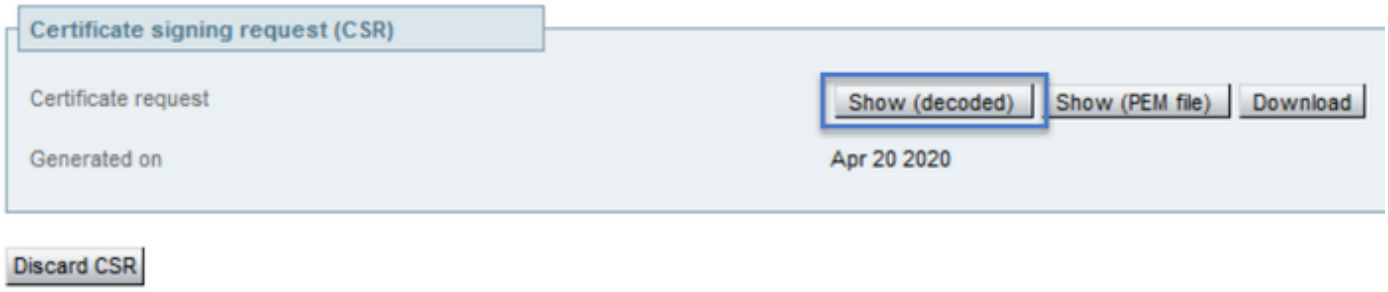
Les **informations supplémentaires** sont requises, si elles ne sont pas autopulées ou doivent être modifiées, elles doivent être entrées manuellement comme indiqué dans l'image :



Une fois terminé, sélectionnez **Générer CSR**.

Étape 3. Vérifiez et téléchargez le nouveau CSR.

Maintenant que le CSR est généré, vous pouvez sélectionner **Show (décodé)** dans la section **CSR (Certificate Sign Request)** pour vérifier que tous les SAN sont présents, comme l'illustre l'image :



Dans la nouvelle fenêtre, recherchez le **CN** et le **Nom alternatif de l'objet** comme indiqué sur l'image :

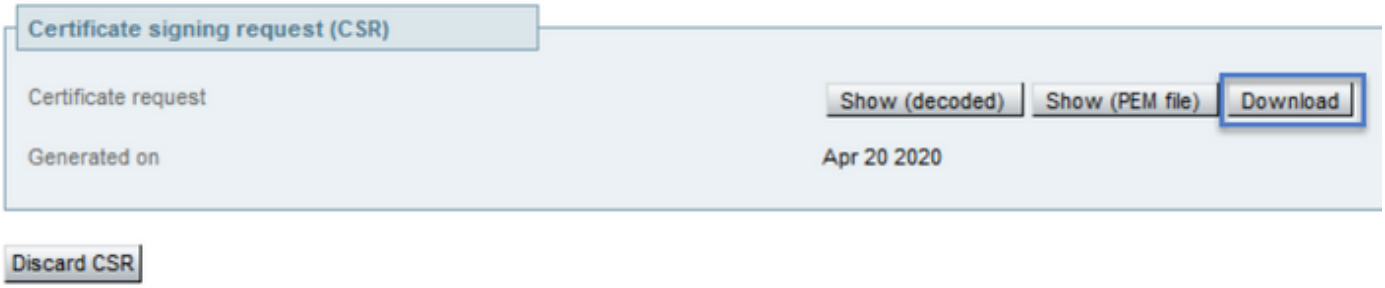
```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: OU=TAC, O=TAC, CN=expe.domain.com, ST=CDMX, C=MX, L=CDMX
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
```

Le CN est toujours ajouté comme SAN automatiquement :

```
        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
```

Maintenant que le CSR a été vérifié, vous pouvez fermer la nouvelle fenêtre et sélectionner

Télécharger (décodé) dans la section **Demande de signature de certificat (CSR)** comme indiqué dans l'image :

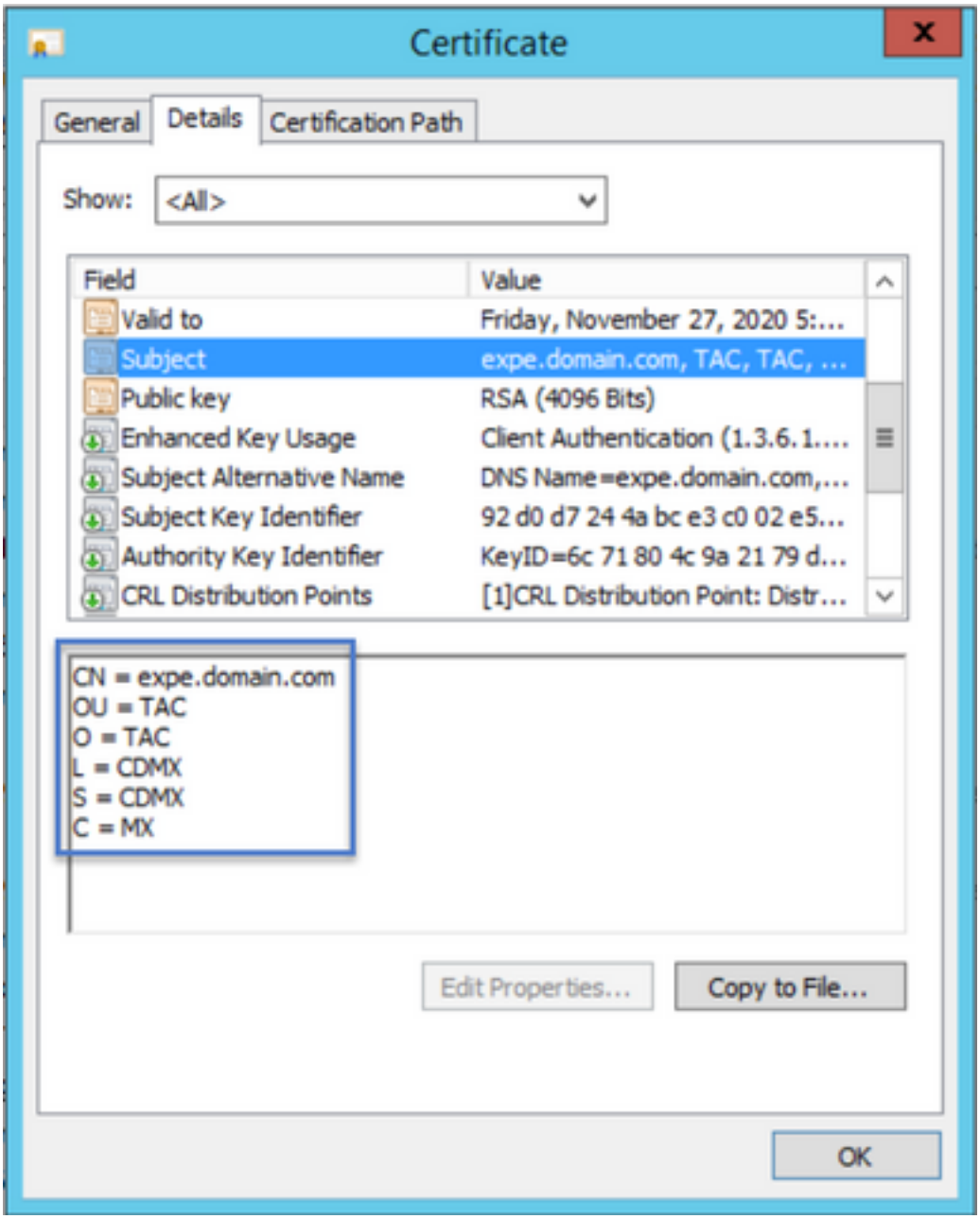


Une fois téléchargé, vous pouvez envoyer le nouveau CSR à votre autorité de certification (CA) à signer.

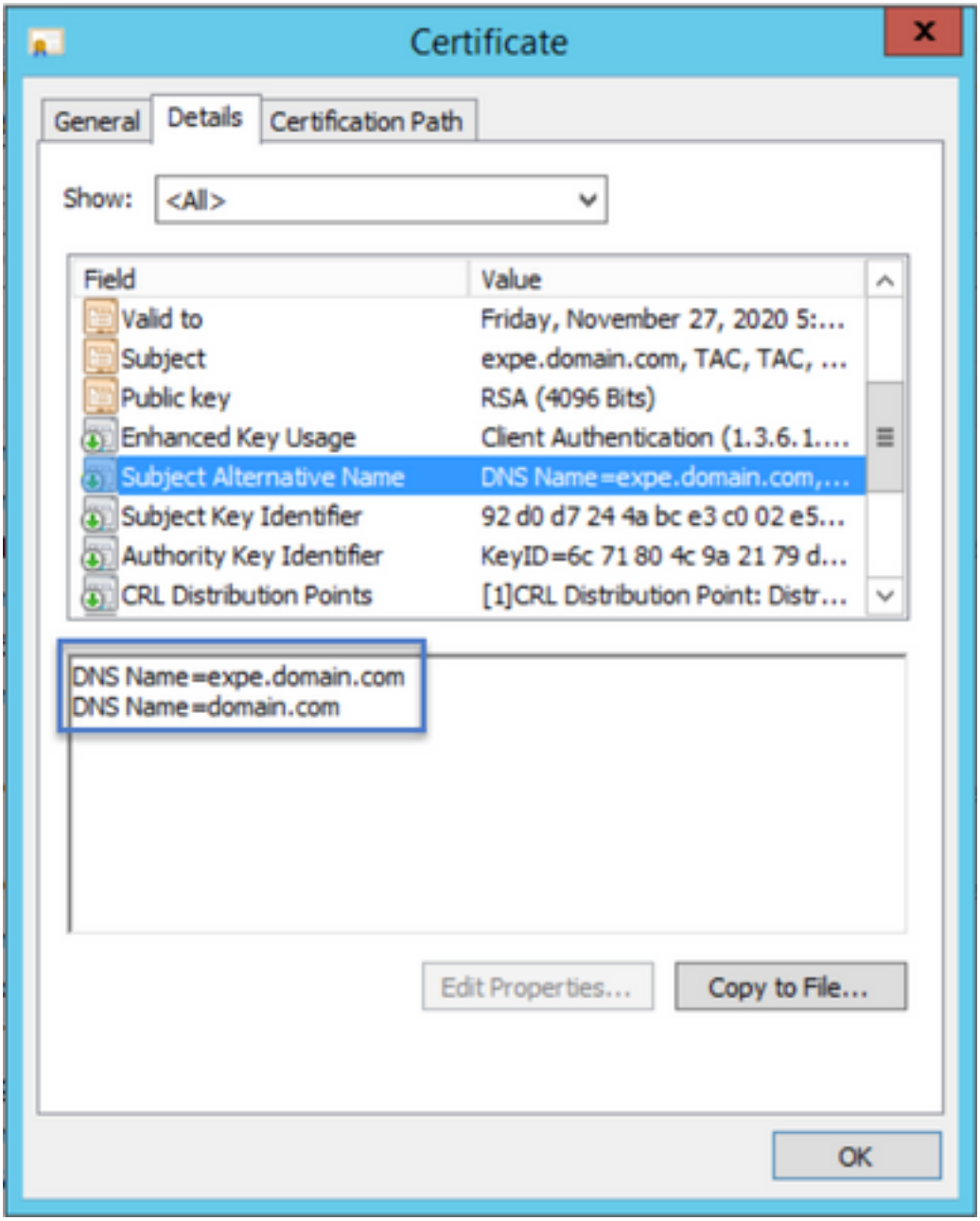
Étape 4. Vérifiez les informations contenues dans le nouveau certificat.

Une fois le nouveau certificat retourné par l'autorité de certification, vous pouvez vérifier si tous les SAN sont présents dans le certificat. Pour ce faire, vous pouvez ouvrir le certificat et rechercher les attributs SAN. Dans ce document, un PC Windows est utilisé pour afficher les attributs, ce n'est pas la seule méthode tant que vous pouvez ouvrir ou décoder le certificat pour vérifier les attributs.

Ouvrez le certificat et accédez à l'onglet **Détails** et recherchez **Objet**, il doit contenir le code CN et les informations supplémentaires, comme indiqué sur l'image :



Recherchez également la section **Subject Alternative Name**, qui doit contenir les SAN que vous avez entrés dans le CSR, comme indiqué sur l'image :



Si tous les SAN que vous avez entrés dans le CSR ne sont pas présents dans le nouveau certificat, contactez votre autorité de certification pour voir si des SAN supplémentaires sont autorisés pour votre certificat.

Étape 5. Téléchargez les nouveaux certificats CA sur le magasin de confiance des serveurs, le cas échéant.

Si l'autorité de certification a signé votre ancien certificat Expressway, vous pouvez annuler cette étape. S'il s'agit d'une autre autorité de certification, vous devez télécharger les nouveaux certificats d'autorité de certification dans la liste des autorités de certification de confiance de chacun des serveurs Expressway. Si vous avez des zones TLS (Transport Layer Security) entre les Expressways, par exemple entre un Expressway-C et un Expressway-E, vous devez télécharger les nouvelles CA sur les deux serveurs afin qu'elles puissent se faire confiance.

Pour ce faire, vous pouvez télécharger vos certificats CA un par un. Accédez à **Maintenance > Security > Trusted CA certificate** sur l'Expressway.

1. Sélectionnez **Parcourir.**

2. Dans la nouvelle page, sélectionnez le certificat CA.
3. Sélectionnez **Append CA Certificate (ajouter le certificat de la CA).**

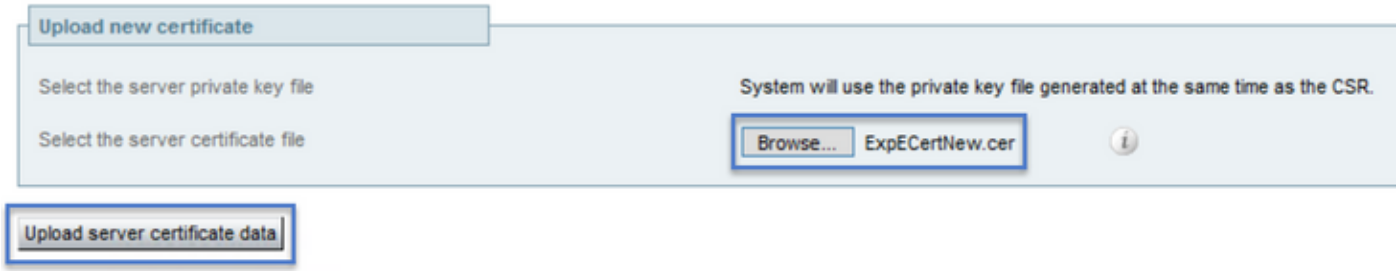
Cette procédure doit être effectuée pour chaque certificat CA de la chaîne de certificats (racine et intermédiaire) et doit être effectuée sur tous les serveurs Expressway même s'ils sont en cluster.

Étape 6. Téléchargez le nouveau certificat sur le serveur Expressway.

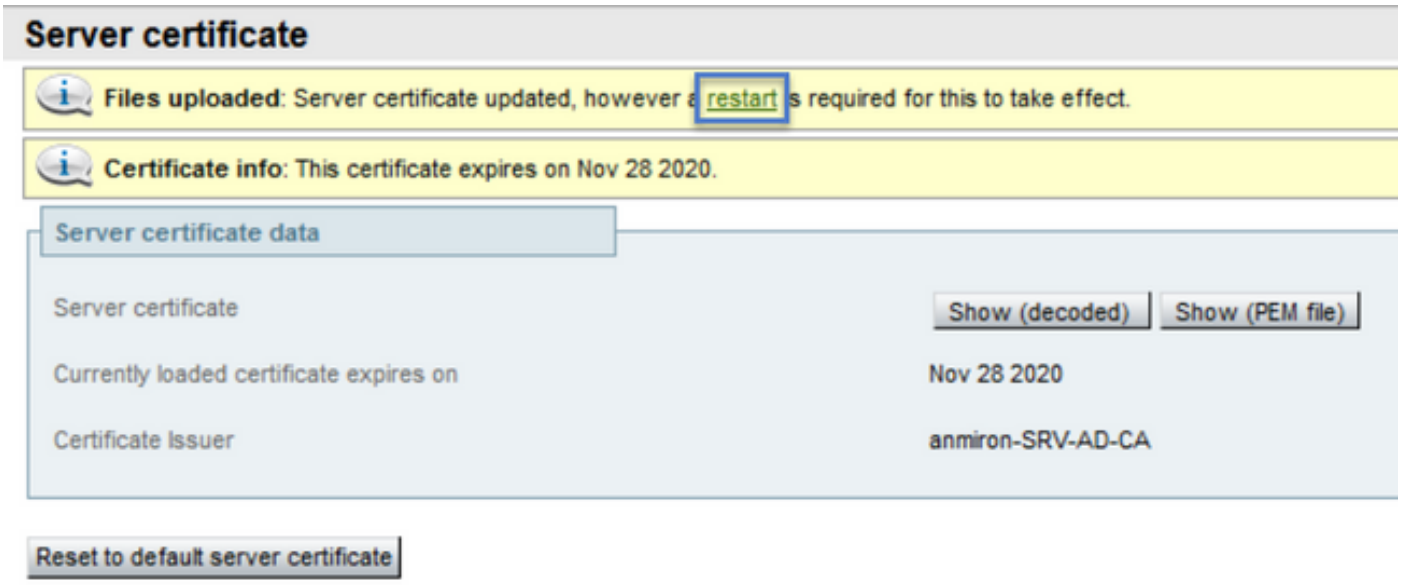
Si toutes les informations du nouveau certificat sont correctes, afin de télécharger le nouveau certificat, accédez à : **Maintenance > Security > Server Certificate.**

Recherchez la section **Télécharger un nouveau certificat** comme indiqué dans l'image :

1. Sélectionnez **Parcourir** dans la section **Sélectionner le fichier de certificat du serveur**.
2. Sélectionnez le nouveau certificat.
3. Sélectionnez **Upload server certificate data (télécharger les données de certificat de serveur).**



Si le nouveau certificat est accepté par l'Expressway, l'Expressway demande un redémarrage pour appliquer les modifications et le message affiche la nouvelle date d'expiration du certificat, comme indiqué sur l'image :

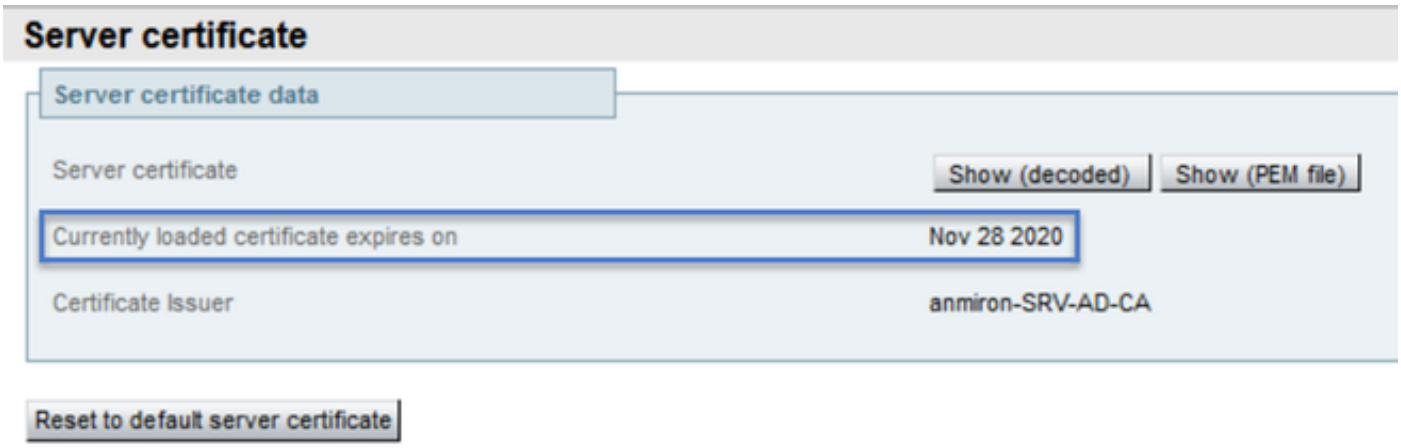


Pour redémarrer l'Expressway, sélectionnez **redémarrer**.

Vérification

Une fois le serveur de nouveau, le nouveau certificat doit avoir été installé, vous pouvez accéder à : **Maintenance > Security > Server Certificate** afin de confirmer.

Recherchez les **données du certificat du serveur** et recherchez le **certificat actuellement chargé expire dans la** section, elle affiche la nouvelle date d'expiration du certificat comme indiqué dans l'image :



Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.