

# Configurer et faire du dépannage pour les certificats Collaboration Edge (MRA)

## Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Autorité de certification publique ou privée \(CA\)](#)

[Fonctionnement des chaînes de certificats](#)

[Résumé de la prise de contact mutuelle SSL](#)

[Configurer](#)

[Zone de traverse/de confiance entre Expressway-C et Expressway-E](#)

[Générer et signer des CSR](#)

[Configurer l'Expressway-C et l'Expressway-E pour qu'ils se fassent confiance](#)

[Communications sécurisée entre Cisco Unified Communications Manager \(CUCM\) et Expressway-C](#)

[Aperçu](#)

[Configurer la confiance entre CUCM et Expressway-C](#)

[Serveurs CUCM avec certificats auto-signés](#)

[Considérations relatives à la grappe Expressway-C et Expressway-E](#)

[Certificats de grappe](#)

[Listes de CA de confiance](#)

[Vérifier](#)

[Vérifier les informations de certificat actuelles](#)

[Lecture/exportation d'un certificat dans Wireshark](#)

[Dépannage](#)

[Tester pour savoir si un certificat est approuvé sur l'Expressway](#)

[Points d'accès Synergy Light \(téléphones de série 7800/8800\)](#)

[Ressources vidéo](#)

[Générer un CSR pour MRA ou Clustered Expressways](#)

[Certificat InstallServer vers Expressway](#)

[Comment configurer l'approbation de certificat entre Expressways](#)

## Introduction

Ce document décrit les certificats en ce qui concerne les déploiements d'accès à distance mobile (MRA).

## Conditions préalables

### Exigences

Aucune exigence spécifique n'est associée à ce document.

### Composants utilisés

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.

## Informations générales

### Autorité de certification (CA) publique c. privée

Il y a un certain nombre d'options de signature de certificats au moyen des serveurs Expressway-C et E. Vous pouvez choisir de faire signer la demande de signature de certificat (CSR) par une autorité de certification publique telle que GoDaddy, Verisign, ou d'autres, ou vous pouvez la signer en interne si vous utilisez votre propre autorité de certification (peut être auto-signée avec OpenSSL ou une autorité de certification d'entreprise interne telle qu'un serveur Microsoft Windows). Pour plus d'informations sur la façon de créer et de signer les CSR utilisés par l'une de ces méthodes, consultez le [Guide de création de certificat du serveur de communication vidéo \(VCS\)](#).

L'Expressway-E est le seul serveur qui doit réellement faire l'objet d'une signature par une autorité de certification publique. Il s'agit du seul serveur où les clients voient le certificat lorsqu'ils se connectent via MRA. Par conséquent, utilisez une autorité de certification publique pour vous assurer que les utilisateurs n'ont pas à accepter manuellement le certificat. L'Expressway-E peut fonctionner avec un certificat interne signé par une autorité de certification, mais les nouveaux utilisateurs seraient invités à accepter le certificat non approuvé. L'enregistrement MRA des téléphones des gammes 7800 et 8800 ne fonctionnerait pas avec les certificats internes car leur liste de certificats de confiance ne peut pas être modifiée. Pour des raisons de simplicité, il est conseillé que vos certificats Expressway-C et Expressway-E soient tous deux signés par la même autorité de certification. Toutefois, cela n'est pas obligatoire tant que vous avez correctement configuré les listes d'autorités de certification approuvées sur les deux serveurs.

### Fonctionnement des chaînes de certificats

Les certificats sont liés ensemble dans une chaîne de deux ou plusieurs éléments utilisés pour vérifier la source qui a signé le certificat du serveur. Il existe trois types de certificats dans une chaîne : le certificat client/serveur, le certificat intermédiaire (dans certains cas) et le certificat racine (également appelé autorité de certification racine car il s'agit de l'autorité de plus haut niveau qui a signé le certificat).

Les certificats contiennent deux champs principaux qui constituent la chaîne : l'objet et l'émetteur.

Le sujet est le nom du serveur ou l'autorité que représente ce certificat. Dans le cas d'un Expressway-C ou d'un Expressway-E (ou d'autres périphériques de communications unifiées (UC)), il s'agit d'un nom de domaine complet (FQDN).

L'émetteur est l'autorité qui a validé le certificat en question. Étant donné que tout le monde peut signer un certificat (qui inclut le serveur qui a créé le certificat, pour commencer, également appelé certificats auto-signés), les serveurs et les clients ont une liste d'émetteurs ou d'autorités de certification qu'ils considèrent comme authentiques.

Une chaîne de certificats se termine toujours par un certificat racine ou de niveau supérieur auto-signé. À mesure que vous vous déplacez dans la hiérarchie des certificats, chaque certificat a un émetteur différent par rapport à l'objet. Finalement, vous rencontrerez l'autorité de certification racine où l'objet et l'émetteur correspondent. Cela indique qu'il s'agit du certificat de niveau supérieur et, par conséquent, de celui qui doit être approuvé par la liste des autorités de certification approuvées d'un client ou d'un serveur.

### Résumé de la prise de contact mutuelle SSL

Dans le cas de la zone de traversée, l'Expressway-C agit toujours en tant que client tandis que l'Expressway-E est toujours le serveur. L'échange simplifié fonctionne comme indiqué :

Expressway-C	Expressway-E
	-----Client Hello----->
<-----Hello du serveur-----	
<----Certificat du serveur-----	
<----Demande de certificatâ€™	
-----Certificat client----->	

La clé ici est dans l'échange puisque l'Expressway-C initie toujours la connexion, et est donc toujours le client. L'Expressway-E est le premier à envoyer son certificat. Si l'Expressway-C ne peut pas valider ce certificat, il interrompt la connexion et ne peut pas envoyer le sien à l'Expressway-E.

Un autre aspect important à envisager tient aux attributs de l'authentification du client web pour la sécurité de couche de transmission (TLS) et de l'authentification du serveur web TLS sur les certificats. Ces attributs sont déterminés sur l'autorité de certification qui a signé le CSR (si une autorité de certification Windows est utilisée, cela est déterminé par le modèle sélectionné) et indiquent si le certificat est valide dans le rôle du client ou du serveur (ou les deux). Parce que pour un VCS ou un Expressway, il peut être basé sur la situation (il est toujours le même pour une zone de traversée), et le certificat doit avoir à la fois des attributs d'authentification client et serveur.

Les Expressway-C et Expressway-E génèrent une erreur lorsqu'ils sont téléchargés vers un nouveau certificat de serveur, si les deux ne sont pas appliqués.

Si vous n'êtes pas sûr qu'un certificat possède ces attributs, vous pouvez ouvrir les détails du certificat dans un navigateur ou dans votre système d'exploitation, et vérifier la section Utilisation étendue de la clé (voir l'image). Le format peut varier et dépend de la façon dont vous regardez le certificat.

Exemple :

General Details

**Certificate Hierarchy**

ACTIVE DIRECTORY-CA

**Certificate Fields**

- Extended Key Usage
- Certificate Subject Alt Name
- Certificate Subject Key ID
- Certificate Authority Key Identifier
- CRL Distribution Points
- Authority Information Access
- Object Identifier (1.3.6.1.4.1.311.21.7)
- Object Identifier (1.3.6.1.4.1.311.21.10)

**Field Value**

Not Critical  
TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)  
TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)

Export...

## Configurer

### Zone de traverse/de confiance entre Expressway-C et Expressway-E

#### Produire et signer des CSR

Comme décrit précédemment, les certificats Expressway-C et Expressway-E doivent être signés par une autorité de certification interne ou externe ou par OpenSSL pour s'auto-signer.

---

**Remarque :** vous ne pouvez pas utiliser le certificat temporaire fourni sur le serveur Expressway, car il n'est pas pris en charge. Si vous utilisez des certificats génériques dans lesquels vous avez un certificat de signature d'autorité de certification et que la ligne d'objet n'est pas spécifiquement définie, elle n'est pas prise en charge.

---

La première étape consiste à générer un CSR et à veiller à sa signature par le type de CA préférée. Le processus pour le faire est précisé dans le guide de création de certificats. Lors de la création du CSR, il est important de garder à l'esprit les noms secondaires de sujet (SAN) nécessaires qui doivent être inclus dans les certificats. Cela est également décrit dans le guide de certificats et dans le guide de déploiement de l'accès mobile à distance. Vérifiez les versions les plus récentes du guide, car vous pouvez en ajouter d'autres à mesure que de nouvelles fonctionnalités arrivent. Liste des réseaux SAN courants à inclure, en

fonction des fonctionnalités utilisées :

#### Expressway-C

- Tous les domaines (internes ou externes) ajoutés à la liste des domaines.
- Tous les alias de noeud de conversation permanente si la fédération XMPP est utilisée.
- Sécurisez les noms de profil de périphérique sur CUCM si des profils de périphérique sécurisés sont utilisés.

#### Expressway-E

- Les domaines configurés sur l'Expressway-C.
- Tous les alias de noeud de conversation permanente si la fédération XMPP est utilisée.
- Les domaines annoncés pour des fédérations XMPP.

---

**Remarque** : si le domaine de base utilisé pour les recherches d'enregistrements de service externes (SRV) n'est pas inclus en tant que SAN dans le certificat Expressway-E (xxx.com ou collab-edge.xxx.com), les clients Jabber exigent toujours que l'utilisateur final accepte le certificat sur la première connexion et les terminaux TC ne parviendraient pas à se connecter du tout.

---

### Configurer l'Expressway-C et l'Expressway-E pour qu'ils se fassent confiance

Pour que la zone de traversée des communications unifiées puisse établir une connexion, Expressway-C et Expressway-E doivent se faire confiance pour leurs certificats respectifs. Pour cet exemple, supposons que le certificat Expressway-E a été signé par une autorité de certification publique qui utilise cette hiérarchie.

Certificat 3

Émetteur : Autorité de certification racine GoDaddy

Objet : Autorité de certification racine GoDaddy

Certificat 2

Émetteur : Autorité de certification racine GoDaddy

Objet : Autorité intermédiaire GoDaddy

Certificat 1

Émetteur : GoDaddy Intermediate Authority

Objet : Expressway-E.lab

L'Expressway-C doit être configuré avec le certificat de confiance 1. Dans la plupart des cas, en fonction des certificats approuvés appliqués au serveur, il envoie uniquement son certificat de serveur de niveau le plus bas. Cela signifie que pour que l'Expressway-C approuve le certificat 1, vous devez télécharger les certificats 2 et 3 dans la liste des autorités de certification approuvées de l'Expressway-C (**Maintenance > Sécurité > Liste des autorités de certification approuvées**). Si vous omettez le certificat intermédiaire 2 lorsque l'Expressway-C reçoit le certificat de l'Expressway-E, il ne peut pas avoir de moyen de le lier à l'autorité de certification racine GoDaddy approuvée, par conséquent il sera rejeté.

Certificat 3

Émetteur : Autorité de certification racine GoDaddy

Objet : Autorité de certification racine GoDaddy

Certificat 1.

Émetteur : Autorité intermédiaire GoDaddy - Non fiable !

Objet : Expressway-E.lab

De plus, si vous téléchargez seulement le certificat intermédiaire sans la racine vers la liste CA approuvée de l'Expressway-C, il verrait que l'Autorité intermédiaire GoDaddy est approuvée, mais qu'elle est signée par une autorité supérieure, dans ce cas, l'Autorité de certification racine GoDaddy qui n'est pas approuvée, par conséquent elle échouera.

Certificat 2.

Émetteur : Autorité de certification racine GoDaddy - Non approuvée !

Objet : Autorité intermédiaire GoDaddy

Certificat 1.

Émetteur : GoDaddy Intermediate Authority

Objet : Expressway-E.lab

Étant donné que tous les certificats intermédiaires et de niveau racine sont ajoutés à la liste des CA de confiance, il est possible de vérifier le certificat...

Certificat 3.

Émetteur : Autorité de certification racine GoDaddy - Le certificat de niveau supérieur auto-signé est approuvé et la chaîne est terminée !

Objet : Autorité de certification racine GoDaddy

Certificat 2.

Émetteur : Autorité de certification racine GoDaddy

Objet : Autorité intermédiaire GoDaddy

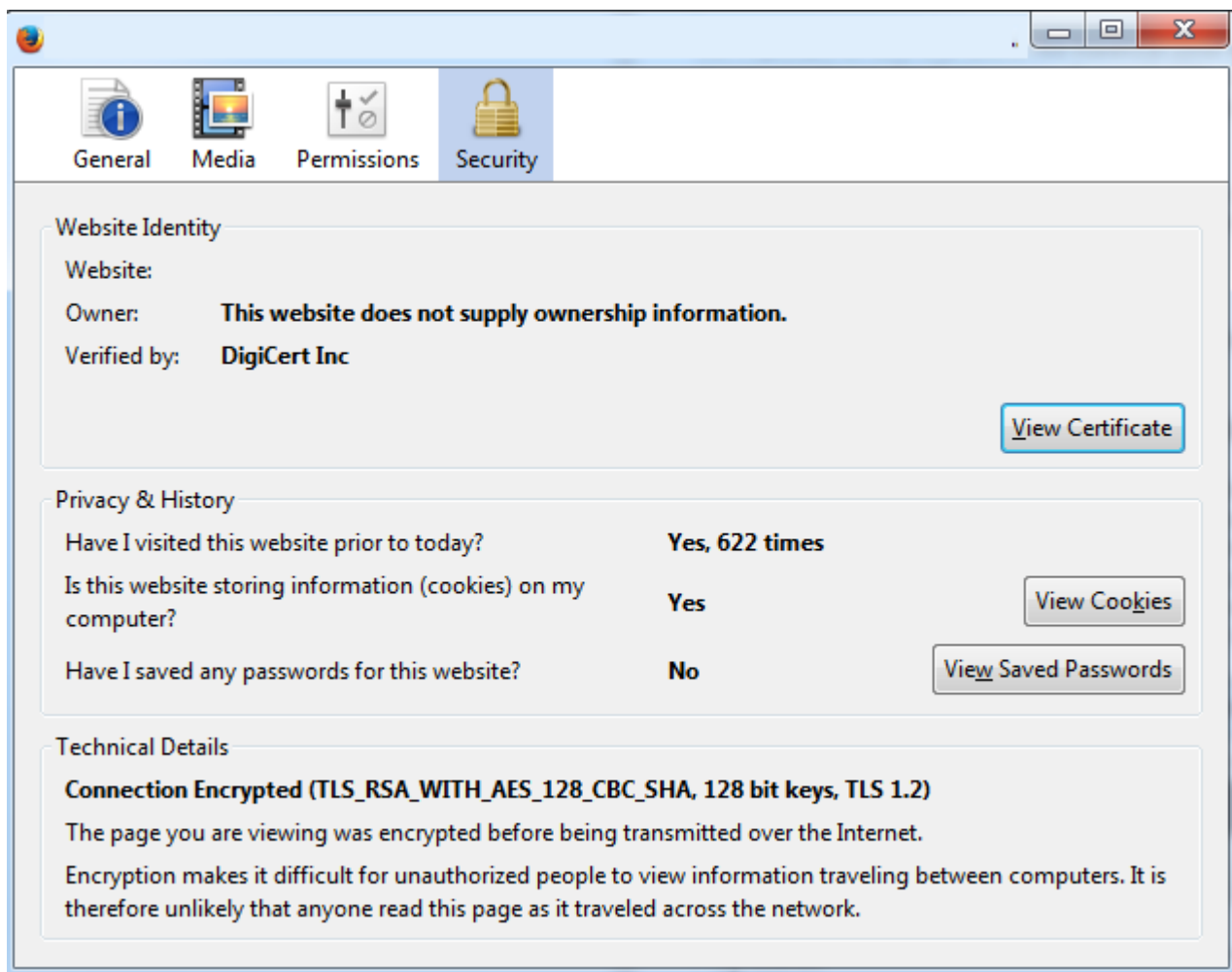
Certificat 1.

Émetteur : GoDaddy Intermediate Authority

Objet : Expressway-E.lab

Si vous n'êtes pas sûr de la chaîne de certificats, vous pouvez vérifier votre navigateur lorsque vous êtes connecté à l'interface Web de l'Expressway spécifique. Le processus varie légèrement en fonction

de votre navigateur, mais dans Firefox, vous pouvez cliquer sur l'icône de verrouillage à l'extrême gauche de la barre d'adresse. Ensuite, dans la fenêtre contextuelle, cliquez sur **Plus d'informations**, > **Voir le certificat** > **Détails**. Si votre navigateur peut assembler la chaîne complète, vous pouvez voir la chaîne de haut en bas. Si l'objet et l'émetteur du certificat de niveau supérieur ne correspondent pas, cela signifie que la chaîne n'est pas terminée. Vous pouvez également exporter chaque certificat de la chaîne par eux-mêmes, si vous cliquez sur **export** avec le certificat souhaité mis en surbrillance. Cette fonctionnalité est utile si vous n'êtes pas parfaitement convaincu d'avoir téléchargé les certificats appropriés dans la liste d'autorités de certification de confiance.



General Details

**This certificate has been verified for the following uses:**

SSL Client Certificate

SSL Server Certificate

**Issued To**

Common Name (CN)

Organization (O)

Organizational Unit (OU)

Serial Number

**Issued By**

Common Name (CN) DigiCert SHA2 High Assurance Server CA

Organization (O) DigiCert Inc

Organizational Unit (OU)

**Period of Validity**

Begins On 3/25/2015

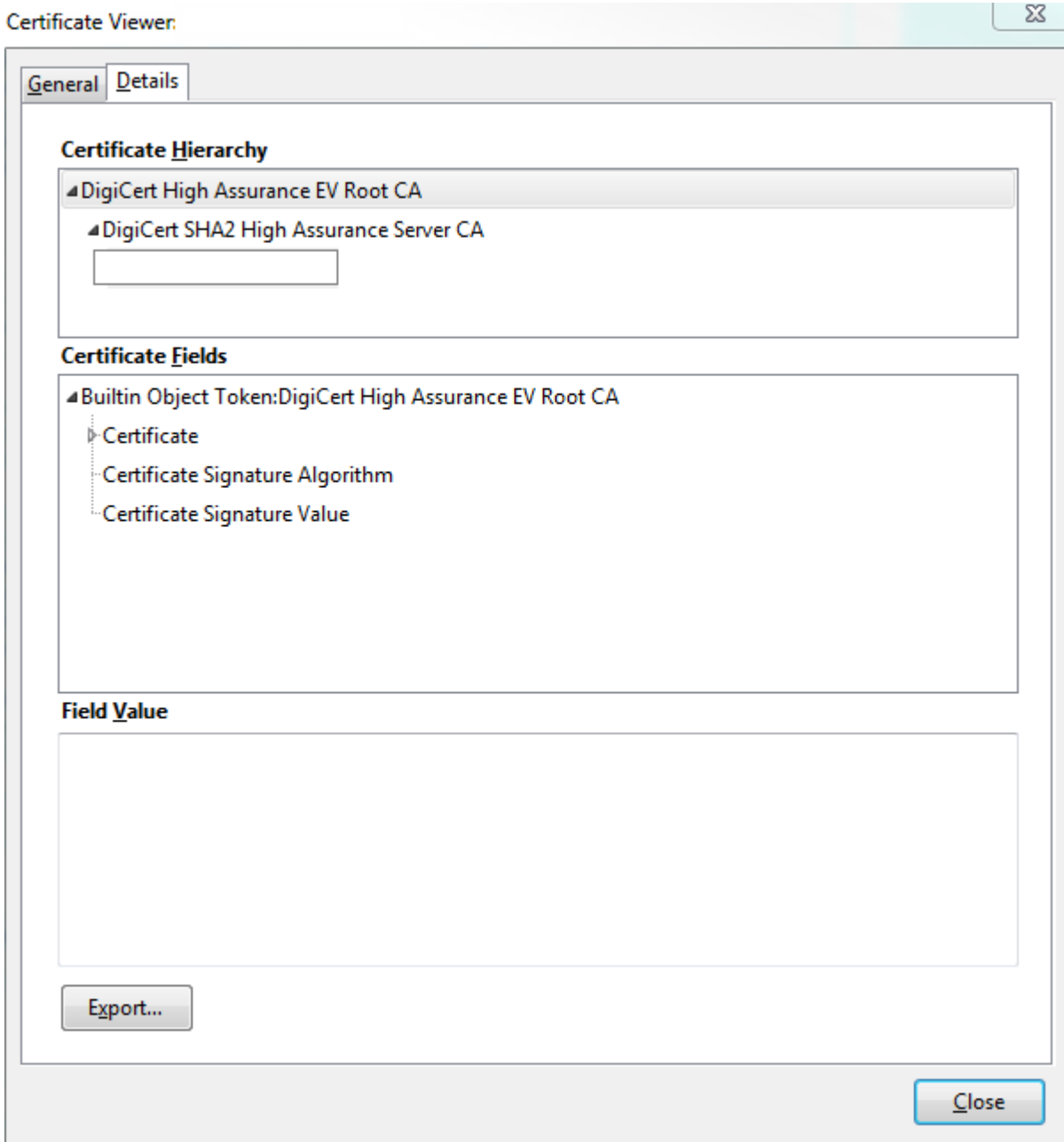
Expires On 4/12/2017

**Fingerprints**SHA-256 Fingerprint 3B:37:23:04:BE:92:0C:FF:2D:48:0B:52:07:5C:D5:08:  
F3:75:F6:0D:43:98:8B:73:22:A4:ED:A8:E6:D7:2A:23

SHA1 Fingerprint CE:7B:79:41:94:9E:07:48:F3:A4:B4:07:03:76:D3:52:12:5D:A9:42

Close





Maintenant que l'Expressway-C fait confiance au certificat de l'Expressway-E, assurez-vous qu'il fonctionne dans la direction opposée. Si le certificat de l'Expressway-C est signé par la même autorité de certification que celle qui a signé l'Expressway-E, le processus est simple. Téléchargez les mêmes certificats dans la liste Autorités de certification de confiance de l'Expressway-E que ceux que vous avez déjà téléchargés sur l'Expressway-E. Si le certificat C est signé par une autre autorité de certification, vous devez utiliser le même processus que celui illustré dans l'image, mais utiliser la chaîne du certificat Expressway-C signé à la place.

## Communications sécurisée entre Cisco Unified Communications Manager (CUCM) et Expressway-C

### Aperçu

Contrairement à la zone de traversée entre Expressway-C et Expressway-E, la signalisation sécurisée n'est PAS requise entre Expressway-C et CUCM. À moins que cela ne soit pas autorisé par les stratégies de sécurité internes, vous devez toujours configurer MRA pour qu'il fonctionne avec des profils de périphériques non sécurisés sur CUCM avant de poursuivre cette étape.

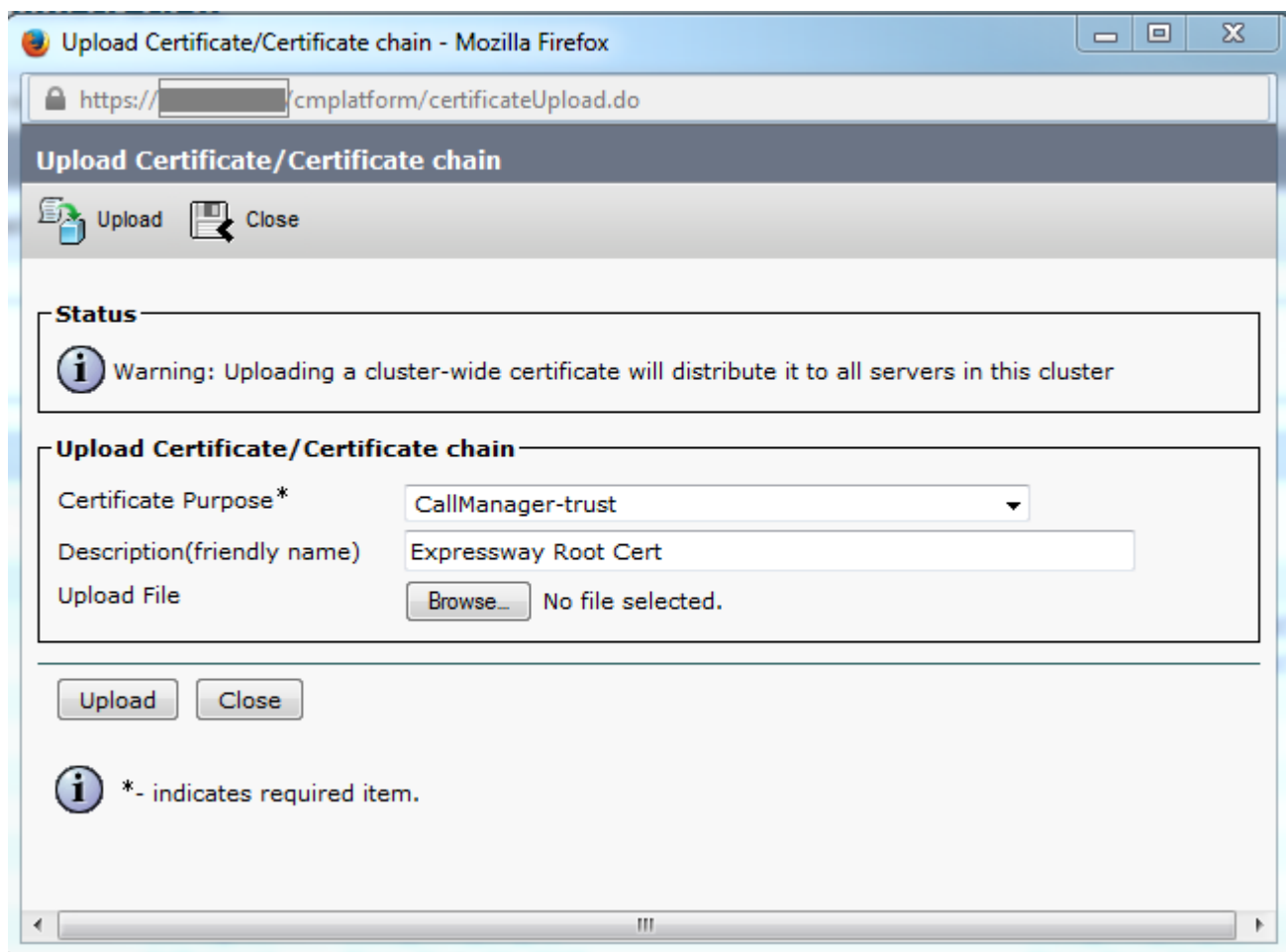
Deux fonctions de sécurité principales peuvent être activées entre CUCM et Expressway-C : TLS Verify et Secure Device Registration. Il y a une importante distinction à établir entre ces deux fonctions, qui font appel à deux différents certificats provenant de CUCM dans la prise de contact mutuelle.

TLS Verify → certificat Tomcat

Secure SIP Registrations → certificat Callmanager

### Configurer la confiance entre CUCM et Expressway-C

Le concept, dans ce cas, est exactement le même qu'entre Expressway-C et Expressway-E. Le CUCM doit d'abord tenir pour fiable le certificat du serveur de Expressway-C. Cela signifie que sur le CUCM, les certificats intermédiaires et racine de Expressway-C doivent être téléchargés en tant que certificat tomcat-trust pour la fonctionnalité de vérification TLS et en tant que certificat CallManager-trust pour les enregistrements de périphériques sécurisés. Pour ce faire, accédez à **Cisco Unified OS Administration** dans le coin supérieur droit de l'interface utilisateur graphique Web de CUCM, puis **Security > Certificate Management**. Ici, pour télécharger un certificat ou une chaîne de certificats, vous pouvez cliquer sur Upload Certificate/Certificate Chain et sélectionner le format de confiance correct ou cliquer sur Find (trouver) pour voir la liste des certificats actuellement téléchargés.



Upload Certificate/Certificate chain - Mozilla Firefox

https://[redacted]/cmplatform/certificateUpload.do

### Upload Certificate/Certificate chain

Upload Close

**Status**

*i* Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

**Upload Certificate/Certificate chain**

Certificate Purpose\* CallManager-trust

Description(friendly name) Expressway Root Cert

Upload File Browse... No file selected.

Upload Close

*i* \*- indicates required item.

Vous devez vous assurer que Expressway-C fait confiance à l'autorité de certification qui a signé les certificats CUCM. Cela peut être réalisé si vous les ajoutez à la liste des autorités de certification de confiance. Dans presque tous les cas, si vous avez signé les certificats CUCM avec une autorité de certification, les certificats tomcat et CallManager doivent être signés par la même autorité de certification. S'ils sont différents, vous devez faire confiance aux deux si vous utilisez TLS Verify et Secure Registrations.

Pour les enregistrements SIP sécurisés, vous devez également vous assurer que le nom de profil de

périphérique sécurisé sur le CUCM qui est appliqué au périphérique est listé comme SAN sur le certificat Expressway-C. Si ce message ne contient pas les messages du registre sécurisé, il échouera avec un 403 du CUCM, ce qui indique un échec de TLS.

---

**Remarque** : lorsque la connexion SSL a lieu entre CUCM et Expressway-C pour un enregistrement SIP sécurisé, deux connexions ont lieu. Tout d'abord, l'Expressway-C agit en tant que client et initie la connexion avec le CUCM. Une fois que cela a été effectué avec succès, CUCM initie une autre connexion en tant que client à répondre. Cela signifie que tout comme l'Expressway-C, le certificat de CallManager sur CUCM doit avoir les attributs d'authentification de client Web de TLS et de serveur Web de TLS. La différence est que le CUCM permet de télécharger ces certificats sans les deux, et les enregistrements sécurisés internes fonctionneraient correctement si le CUCM n'a que l'attribut d'authentification du serveur. Vous pouvez le confirmer sur CUCM si vous recherchez le certificat CallManager dans la liste et que vous le sélectionnez. Là, vous pouvez consulter les oids d'utilisation sous la section Extension. Vous pouvez voir 1.3.6.1.5.5.7.3.2 pour l'authentification du client et 1.3.6.1.5.5.7.3.1 pour l'authentification du serveur. Vous pouvez également télécharger le certificat dans cette fenêtre.

---

Certificate Details(CA-signed) - Mozilla Firefox

https://[redacted]/cmplatform/certificateEdit.do?cert=/usr/local/cm/.security/CallManager/certs/CallManager.pem

### Certificate Details for cucm10-lab-pub.tkratzke.local, CallManager

Regenerate
 Generate CSR
 Download .PEM File
 Download .DER File

---

**Status**

Status: Ready

---

**Certificate Settings**

Locally Uploaded	01/04/15
File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Certificate Signed by tkratzke-ACTIVEDIRECTORY-CA

---

**Certificate File Data**

```

Key: RSA (1.2.840.113549.1.1.1)
  Key value:
3082010a0282010100c3f0061dafbffa97cd781c9627134664cae9f55d5d92871b60ce17ddf78972963a4
1db705c43c97046df73897748e2a2459c96f7cd3cc849c71055b27ffd30dc6d4ebc727beb7a96e98ab78
01d25eb0e354086e318df242d4039004f2c569308c875697ecdf2b9040d4aa22da5b7a82f667abbd2342
0fe820dd157a648ee4c611ca8612cef49f35dd8e01677b18edca260c6aa3920da979e4adadb7ed4c776e
e1c9a28d9eaf90648cafaf757a7050ec0fc383eccbb227d0947e3265737f640e7db4d280e477689ba395
60a6a39db010fad4e2da05beea5c8f47357726d90e56c1415c499e8d09ab36357c1223f1bae52baa82
32ba70485bd745407b354bd09d0203010001
  Extensions: 9 present
  [
    Extension: ExtKeyUsageSyntax (OID.2.5.29.37)
    Critical: false
    Usage oids: 1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.1,
  ]
  [
  ]
  
```

**Remarque** : les certificats d'approbation appliqués à l'éditeur dans un cluster doivent être répliqués sur les abonnés. Il est bon de confirmer en se connectant à eux séparément sur une nouvelle configuration.

**Remarque** : pour que l'Expressway-C valide correctement le certificat de CUCM, les serveurs CUCM DOIVENT être ajoutés à l'Expressway-C avec le nom de domaine complet et non l'adresse IP. La seule façon dont l'adresse IP peut fonctionner est si l'adresse IP de chaque noeud CUCM est ajoutée en tant que SAN dans le certificat, ce qui n'est presque jamais fait.

## Serveurs CUCM avec certificats auto-signés

Par défaut, un serveur CUCM est fourni avec des certificats auto-signés. S'ils sont en place, il n'est pas possible d'utiliser simultanément TLS Verify et Secure Device Registration. Chaque fonctionnalité peut être utilisée seule, mais comme les certificats sont auto-signés, cela signifie que les certificats Tomcat et CallManager auto-signés doivent être téléchargés vers la liste de CA de confiance sur l'Expressway-C. Lorsque Expressway-C effectue une recherche dans sa liste de confiance pour valider un certificat, il s'arrête dès qu'il en trouve un avec un objet correspondant. Pour cette raison, si la valeur la plus élevée de la liste de confiance est tomcat ou CallManager, cette fonctionnalité fonctionnera. La plus basse échouerait comme si elle n'était pas présente. Pour surmonter cette difficulté, il faut signer les certificats de CUCM avec une autorité de certification (CA) (publique ou privée) et faire confiance seulement à cette autorité de certification.

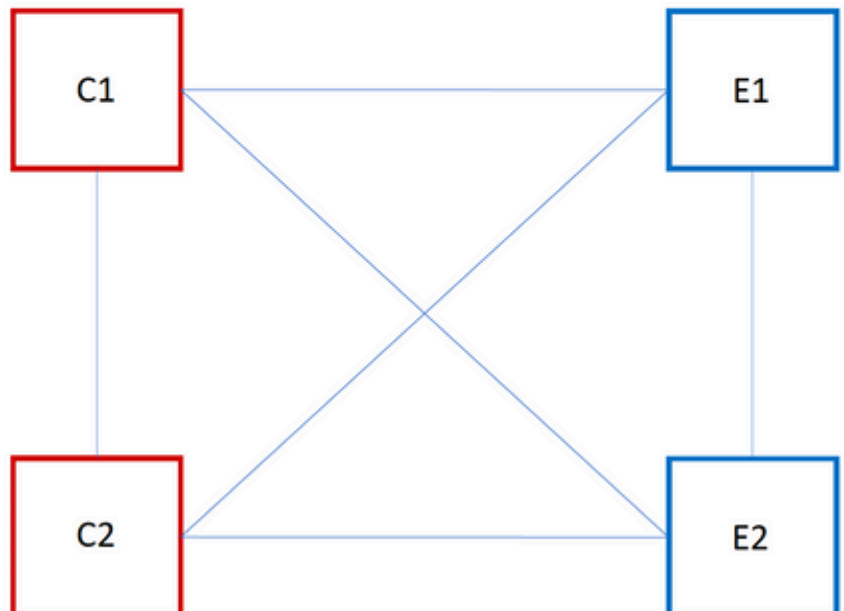
## Considérations relatives à la grappe Expressway-C et Expressway-E

### Certificats de grappe

Si vous avez une grappe de serveurs Expressway-C ou Expressway-E pour la redondance, il est vivement recommandé que vous produisiez une demande distincte de signature de certificat pour chaque serveur en veillant à obtenir la signature d'une CA. Dans le scénario précédent, le nom commun (CN) de chaque certificat d'homologue serait le même nom de domaine complet (FQDN) de cluster et les réseaux SAN seraient le nom de domaine complet de cluster et le nom de domaine complet d'homologue respectif, comme indiqué dans l'image :

## Expressway Cluster Certificate MRA

CN: FQDN of CLUSTER  
SAN: FQDN C1 AND CLUSTER FQDN  
SAN: PHONE SECURITY PROFILE  
(FQDN FORMAT)(If Configured on CUCM)

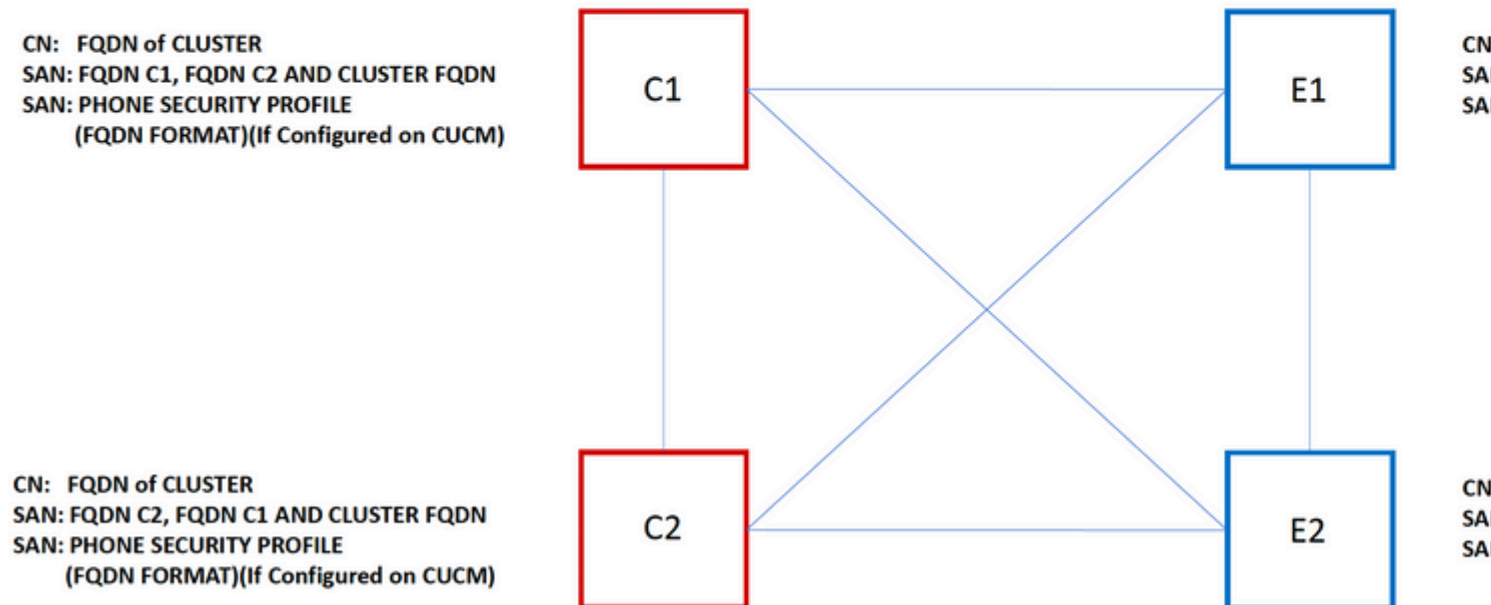


CN: FQDN of CLUSTER  
SAN: FQDN C2 AND CLUSTER FQDN  
SAN: PHONE SECURITY PROFILE  
(FQDN FORMAT)(If Configured on CUCM)

Vous pouvez utiliser le nom de domaine complet du cluster comme nom de domaine complet du cluster et chaque nom de domaine complet de l'homologue et du cluster dans le SAN pour utiliser le même certificat pour tous les noeuds du cluster, et éviter ainsi le coût de plusieurs certificats signés par une autorité de certification publique.

# Expressway Cluster Certificates

## MRA



**Remarque :** les noms de profil de sécurité téléphonique du certificat Cs ne sont requis que si vous utilisez des profils de sécurité téléphonique sécurisés sur l'UCM. Le domaine externe ou collab-edge.example.com (où example.com est votre domaine) est une condition requise uniquement pour l'enregistrement du téléphone IP et du terminal TC sur MRA. Cette option est facultative pour l'enregistrement Jabber sur MRA. S'il n'est pas présent, jabber vous invite à accepter le certificat lorsque jabber se connecte via MRA.

Si cela est absolument nécessaire, cela peut être fait avec le processus suivant ou vous pouvez utiliser OpenSSL pour générer à la fois la clé privée et la CSR manuellement :

Étape 1. Générez un CSR sur le noeud principal du cluster et configurez-le pour répertorier l'alias de cluster en tant que CN. Ajoutez tous les homologues dans la grappe sous forme d'autres noms (alternative names), avec tous les autres SAN requis.

Étape 2. Signez ce CSR et téléchargez-le sur l'homologue principal.

Étape 3. Connectez-vous au serveur principal en tant que racine et téléchargez la clé privée située dans /Tandberg/persistent/certs.

Étape 4. Téléchargez à la fois le certificat signé et la clé privée correspondante vers chaque homologue du cluster.

**Remarque :** ceci n'est pas recommandé pour les raisons suivantes :

1. Il s'agit d'un risque de sécurité car tous les homologues utilisent la même clé privée. Si l'un d'entre eux est compromis, un pirate peut déchiffrer le trafic provenant de n'importe quel serveur.

---

2. Si une modification doit être apportée au certificat, il faudra effectuer le processus en entier de nouveau, au lieu de simplement produire et signer la CSR.

---

## Listes de CA de confiance

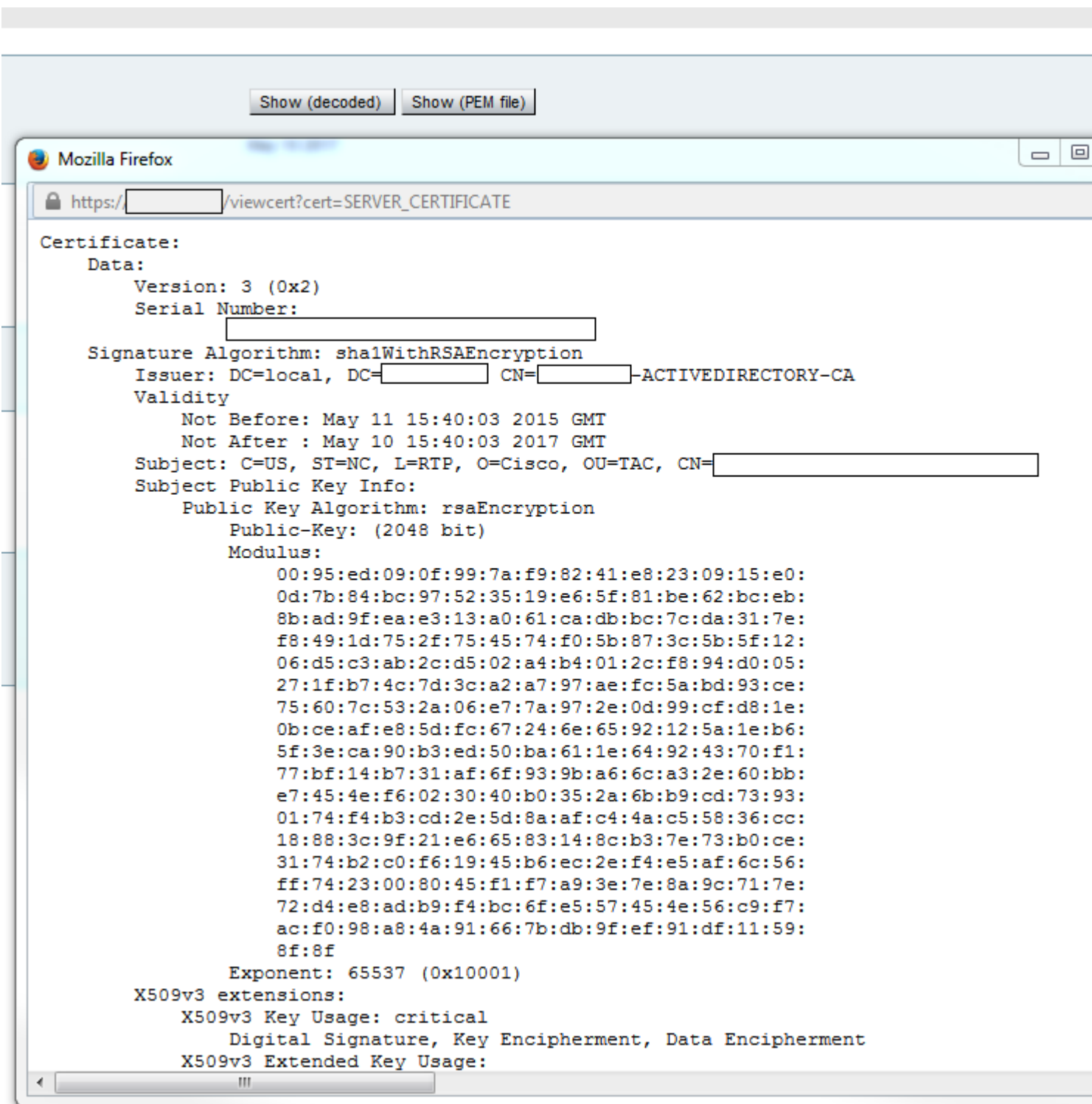
À la différence des abonnés CUCM dans une grappe, la liste de CA de confiance n'est PAS reproduite entre les homologues d'une grappe VCS ou Expressway. Cela signifie que si vous disposez d'un cluster, vous devez télécharger manuellement des certificats approuvés dans la liste d'autorités de certification de chaque homologue.

## Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

### Vérifier les informations de certificat actuelles

Il y a plusieurs façons de vérifier les renseignements d'un certificat existant. La première option est via le navigateur Web. Utilisez la méthode décrite dans la section précédente qui peut également être utilisée pour exporter un certificat spécifique dans la chaîne. Si vous avez besoin de vérifier des SAN, ou d'autres attributs ajoutés au certificat du serveur Expressway, vous pouvez le faire directement par l'interface graphique utilisateur (GUI) Web, naviguez à **Maintenance > Certificats de sécurité > Certificat du serveur**, puis cliquez sur **Show Decoded**.



Ici vous pouvez voir tous les détails spécifiques du certificat sans avoir besoin de le télécharger. Vous pouvez également faire de même pour une demande de signature (CSR) active, si le certificat en cause nâ€™Ma pas encore été téléversé.

## Lecture/exportation d'un certificat dans Wireshark

Si vous disposez d'une capture Wireshark de la connexion SSL qui inclut l'échange de certificats, Wireshark peut en fait décoder le certificat pour vous et vous pouvez en fait exporter tous les certificats de la chaîne (si la chaîne complète est échangée) depuis l'intérieur. Filtrer votre capture de paquets selon le port spécifique de lâ€™TMéchange de certificat (en général, 7001 dans le cas dâ€™TMune zone de traverse). Ensuite, si vous ne voyez pas les paquets Hello du client et du serveur avec la connexion SSL, cliquez avec le bouton droit sur



l'un des paquets dans le flux TCP et sélectionnez **décoder comme**. Sélectionnez **SSL** et cliquez sur **apply**. Maintenant, si vous avez capturé le trafic correct, vous devez voir l'échange de certificats. Recherchez le paquet du serveur correct qui contient le certificat dans la charge utile. Développez la section SSL dans le volet inférieur jusqu'à ce que vous voyiez la liste des certificats comme indiqué dans l'image :

The screenshot shows the Wireshark interface with a filter set to 'tcp.stream eq 19'. The packet list pane shows several packets, with packet 1813 selected. The packet details pane is expanded to show the 'Secure Sockets Layer' section, which includes 'TLSv1.2 Record Layer: Handshake Protocol: Certificate', 'Handshake Protocol: Certificate', and a list of certificates. The selected certificate is 'Certificate (id-at-commonName=..., id-at-organizationalUnitName=...)' with a length of 911 bytes.

No.	Time	Source	Destination	Protocol
1803	2015-06-03 18:01:07.522714			TCP
1806	2015-06-03 18:01:07.522835			TCP
1807	2015-06-03 18:01:07.522855			TCP
1808	2015-06-03 18:01:07.523594			TLS
1809	2015-06-03 18:01:07.523846			TCP
1811	2015-06-03 18:01:07.538935			TLS
1812	2015-06-03 18:01:07.538970			TCP
1813	2015-06-03 18:01:07.539008			TLS

Frame 1813: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface  
 Ethernet II, Src: Vmware\_a1:14:46 ( ), Dst: Vmware\_a1:1e:e1 ( )  
 Internet Protocol Version 4, Src: , Dst: :  
 Transmission Control Protocol, Src Port: 7001 (7001), Dst Port: 443 (443)  
 [2 Reassembled TCP Segments (2541 bytes): #1811(1390), #1813(1151)]  
 Secure Sockets Layer  
 TLSv1.2 Record Layer: Handshake Protocol: Certificate  
 Content Type: Handshake (22)  
 Version: TLS 1.2 (0x0303)  
 Length: 2536  
 Handshake Protocol: Certificate  
 Handshake Type: Certificate (11)  
 Length: 2532  
 Certificates Length: 2529  
 Certificates (2529 bytes)  
 Certificate Length: 1612  
 Certificate (id-at-commonName=..., id-at-organizationalUnitName=...)  
 Certificate Length: 911  
 Certificate (id-at-commonName=...-ACTIVEDIRECTORY-CA, dc=..., dc=...)

Ici, vous pouvez développer n'importe lequel des certificats pour voir tous les détails. Si vous souhaitez exporter le certificat, cliquez avec le bouton droit sur le certificat souhaité dans la chaîne (s'il y en a plusieurs) et sélectionnez **Exporter les octets de paquets sélectionnés**. Entrez un nom pour le certificat et cliquez sur le bouton pour enregistrer (**save**). À présent, vous devez pouvoir ouvrir le certificat dans la Visionneuse de certificats Windows (si vous lui attribuez une extension .cer) ou le télécharger vers tout autre outil d'analyse.

## Dépannage

Cette section fournit les informations que vous pouvez utiliser pour dépanner votre configuration.

### Tester pour savoir si un certificat est approuvé sur l'Expressway

Bien que la meilleure méthode consiste à vérifier manuellement la chaîne de certificats et à s'assurer que tous les membres sont inclus dans la liste des CA de confiance d'Expressway, vous pouvez rapidement vérifier que l'Expressway fait confiance au certificat d'un client spécifique à l'aide de **Client Certificate Testing** sous **Maintenance > Security Certificates** dans l'interface utilisateur graphique Web. Conservez tous les paramètres par défaut. Sélectionnez **Upload Test File** (format pem) dans la liste

déroulante et sélectionnez le certificat client que vous souhaitez vérifier. Si le certificat n'est pas approuvé, vous obtiendrez une erreur, comme indiqué dans l'image, qui explique la raison pour laquelle il a été rejeté. L'erreur que vous voyez est l'information décodée du certificat téléchargé pour référence.

### Client certificate testing

#### Client certificate

This tests whether a client certificate is valid.

Certificate source

Select the file you want to test

Currently uploaded test file

Uploaded test file (PEM format)

No file selected

pm-vcsc01.cer

#### Certificate-based authentication pattern

This section applies only if you are using certificate-based authentication.

Regex to match against certificate

Username format

### Certificate test results

Valid certificate: Invalid: The client certificate is not signed by a CA in the trusted CA list.

Si vous obtenez une erreur qui prétend que l'Expressway n'est pas en mesure d'obtenir la CRL de certificat, mais que l'Expressway n'utilise pas la vérification de la CRL, cela signifie que le certificat serait approuvé et a réussi toutes les autres vérifications de vérification.

## Client certificate testing

### Client certificate

Certificate source

Select the file you want to test

Currently uploaded test file

This tests whether a client cer

Uploaded test file (PEM forma

Browse...

No file selected

vcs.cer

### Certificate-based authentication pattern

Regex to match against certificate

Username format

This section applies only if you

username format combinations

/Subject.\*CN=(?<captureCom

#captureCommonName#

Make these settings perman

Check certificate

## Certificate test results

Valid certificate:

Invalid: unable to get certificate CRL, please ensure that you have uploaded a CRL

## Points d'accès Synergy Light (téléphones de série 7800/8800)

Ces nouveaux périphériques sont livrés avec une liste de certificats de confiance préremplie, qui inclut un grand nombre d'autorités de certification publiques bien connues. Cette liste de confiance ne peut pas être modifiée, ce qui signifie que votre certificat Expressway-E DOIT être signé par une de ces autorités de certification publiques correspondantes afin de fonctionner avec ces périphériques. Si elle est signée par une autorité de certification interne ou une autre autorité de certification publique, la connexion échouera. Il n'y a pas d'option permettant à l'utilisateur d'accepter manuellement le certificat, comme on le voyait avec les clients Jabber.

**Remarque :** il a été constaté pour certains déploiements que l'utilisation d'un périphérique tel que Citrix NetScaler avec une CA de la liste incluse sur les téléphones de la gamme 7800/8800 peut s'enregistrer sur MRA même si l'Expressway-E utilise une CA interne. L'autorité de certification racine NetScalers doit être téléchargée vers l'Expressway-E et l'autorité de certification racine interne doit être téléchargée vers Netscaler pour que l'authentification SSL fonctionne. Il a été démontré que cela fonctionne et qu'il s'agit d'un soutien au mieux.

**Remarque :** si la liste d'autorités de certification de confiance semble contenir tous les certificats corrects, mais qu'elle est toujours rejetée, assurez-vous qu'il n'y a pas d'autre certificat plus haut dans

---

la liste avec le même sujet qui pourrait entrer en conflit avec le bon. Lorsque tout le reste échoue, vous pouvez toujours exporter la chaîne directement à partir du navigateur ou de Wireshark, et télécharger tous les certificats vers la liste d'autorité de certification des serveurs opposés. Cela garantirait qu'il s'agit du certificat de confiance.

---

**Remarque** : lorsque vous dépannez un problème de zone de traversée, le problème peut parfois sembler lié à un certificat, mais il s'agit en fait d'un problème logiciel. Assurez-vous que le nom d'utilisateur et le mot de passe utilisés pour la traverse sont exacts.

---

**Remarque** : le VCS ou l'Expressway ne prend pas en charge plus de 999 caractères dans le champ SAN d'un certificat. Tous les SAN qui dépassent cette limite (qui nécessite de nombreux noms alternatifs) seront ignorés comme s'ils n'étaient pas présents.

---

## Ressources vidéo

Cette section fournit des informations dans la vidéo qui peuvent vous guider tout au long des processus de configuration des certificats.

[Générer un CSR pour MRA ou Clustered Expressways](#)

[Installer le certificat du serveur sur Expressway](#)

[Comment configurer l'approbation de certificat entre Expressways](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.