Exemple basé sur comité de configuration de points finaux de périphérie de Collaboration

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Configurez
Créez un profil téléphonique sécurisé sur CUCM dans le format FQDN (facultatif)
Assurez que security mode de batterie est (1) - Mélangé (facultatif)
Créez un profil dans CUCM pour le point final basé sur comité
Ajoutez le nom de profil de Sécurité au SAN du certificat Expressway-C/VCS-C (facultatif)
Ajoutez le domaine UC au certificat Expressway-E/VCS-E
Installez le certificat de CA de confiance approprié sur le point final basé sur comité
Installez un point final basé sur comité pour le ravitaillement de périphérie
Vérifiez
point final basé sur comité
CUCM
Autoroute-C
Dépannez
Outils
Point final comité technique
Autoroutes
CUCM
Question 1 : l'enregistrement de Collab-périphérie n'est pas visible et/ou l'adresse Internet n'est pas résoluble
Issue 2 : Le CA n'est pas présent dans la liste de confiance CA sur le point final basé sur comité
Question 3 : L'autoroute-e n'a pas le domaine UC répertorié dans le SAN
Question 4 : Le nom d'utilisateur et/ou le mot de passe fournis dans le profil de ravitaillement comité technique est incorrect
Question 5 : L'enregistrement basé sur comité de point final obtient rejeté
Informations connexes

Introduction

Le document décrit ce qui est exigé afin de configurer et dépanner l'enregistrement basé sur de point final des codecs de TelePresence (comité technique) par le mobile et la solution d'accès distant.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Mobile et solution d'accès distant
- Certificats du serveur de communication vidéo (VCS)
- Autoroute X8.1.1 ou plus tard
- Version 9.1.2 du gestionnaire de Cisco Unified Communications (CUCM) ou plus tard
- points finaux basés sur comité

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- VCS X8.1.1 ou plus tard
- Release CUCM 9.1(2)SU1 ou plus tard et IM et présence 9.1(1) ou plus tard
- Comité technique 7.1 ou micrologiciel postérieur **(TC7.2 recommandés)**
- Contrôle VCS et autoroute/noyau et périphérie d'autoroute
- CUCM
- Point final comité technique

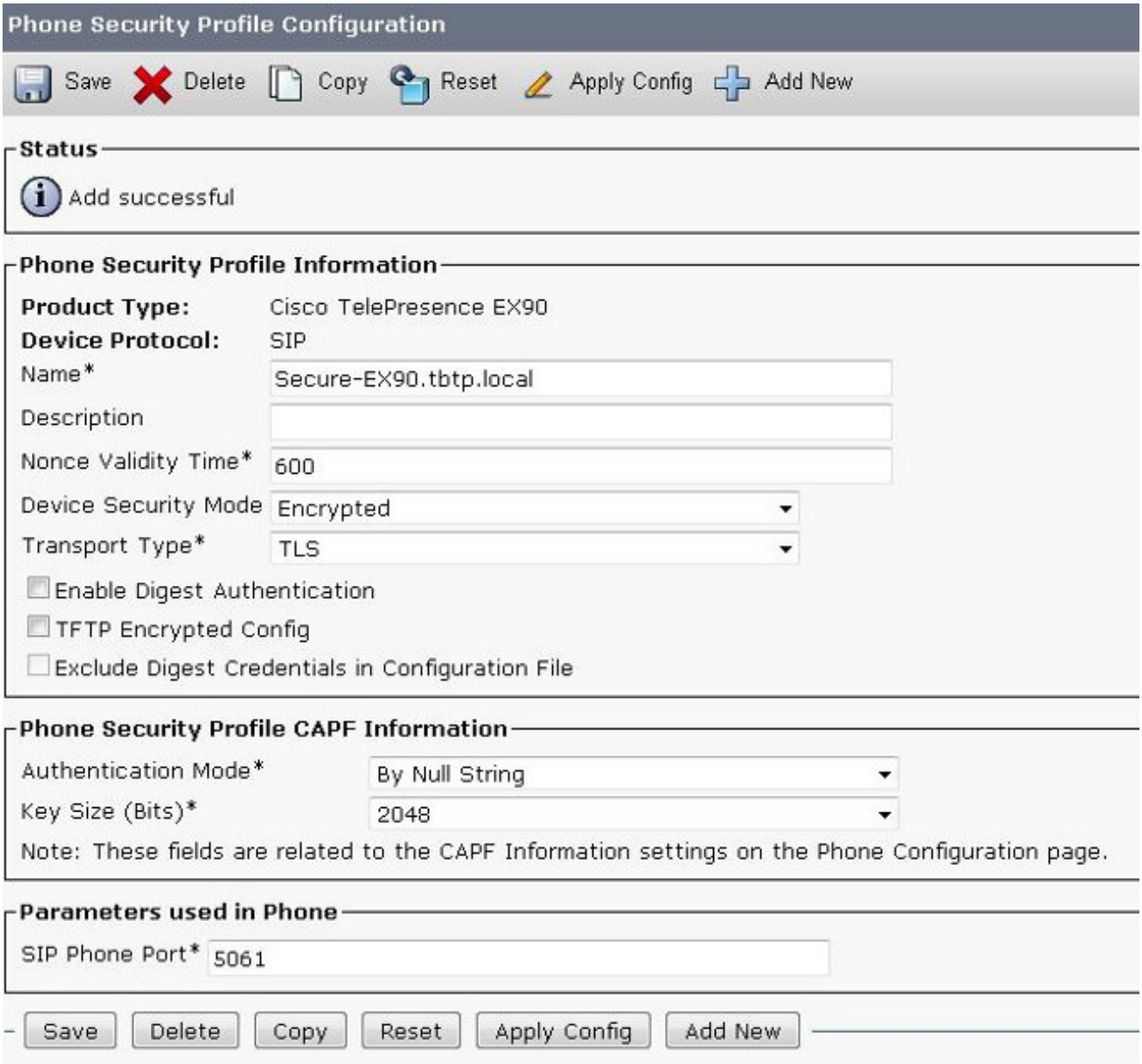
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Ces étapes de configuration supposent que l'administrateur configurera le point final basé sur comité pour sécurisent l'enregistrement de périphérique. L'enregistrement sécurisé n'est pas une condition requise, toutefois le guide global de mobile et de solution d'accès distant donne l'impression qu'il est puisqu'il y a des copies d'écran de la configuration qui affichent des profils de périphérique sécurisés sur CUCM.

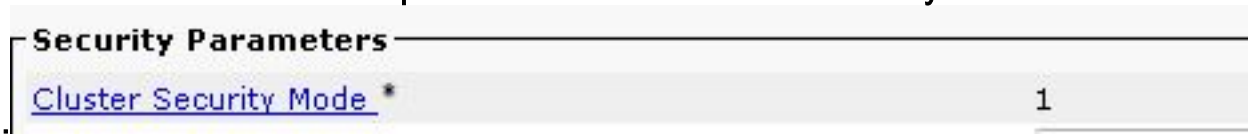
Créez un profil téléphonique sécurisé sur CUCM dans le format FQDN (facultatif)

1. Dans CUCM, **profil** choisi de **système > de Sécurité > de degré de sécurité de téléphone**.
2. Cliquez sur Add **nouveau**.
3. Sélectionnez le type basé sur comité de point final et configurez ces paramètres : Nom - **Secure-EX90.tbtp.local (format FQDN exigé)**Mode de sécurité des périphériques - **Chiffré**Type de transport - **TLS**Port de téléphone SIP - **5061**



Assurez que security mode de batterie est (1) - Mélangé (facultatif)

1. Dans CUCM, **System > Enterprise Parameters** choisi.
2. Faites descendre l'écran aux **paramètres de Sécurité > à la security mode de batterie >**

1. 

Si la valeur n'est pas 1 le CUCM n'a pas été sécurisé. Si c'est le cas, l'administrateur doit examiner un de ces deux documents afin de sécuriser le CUCM.

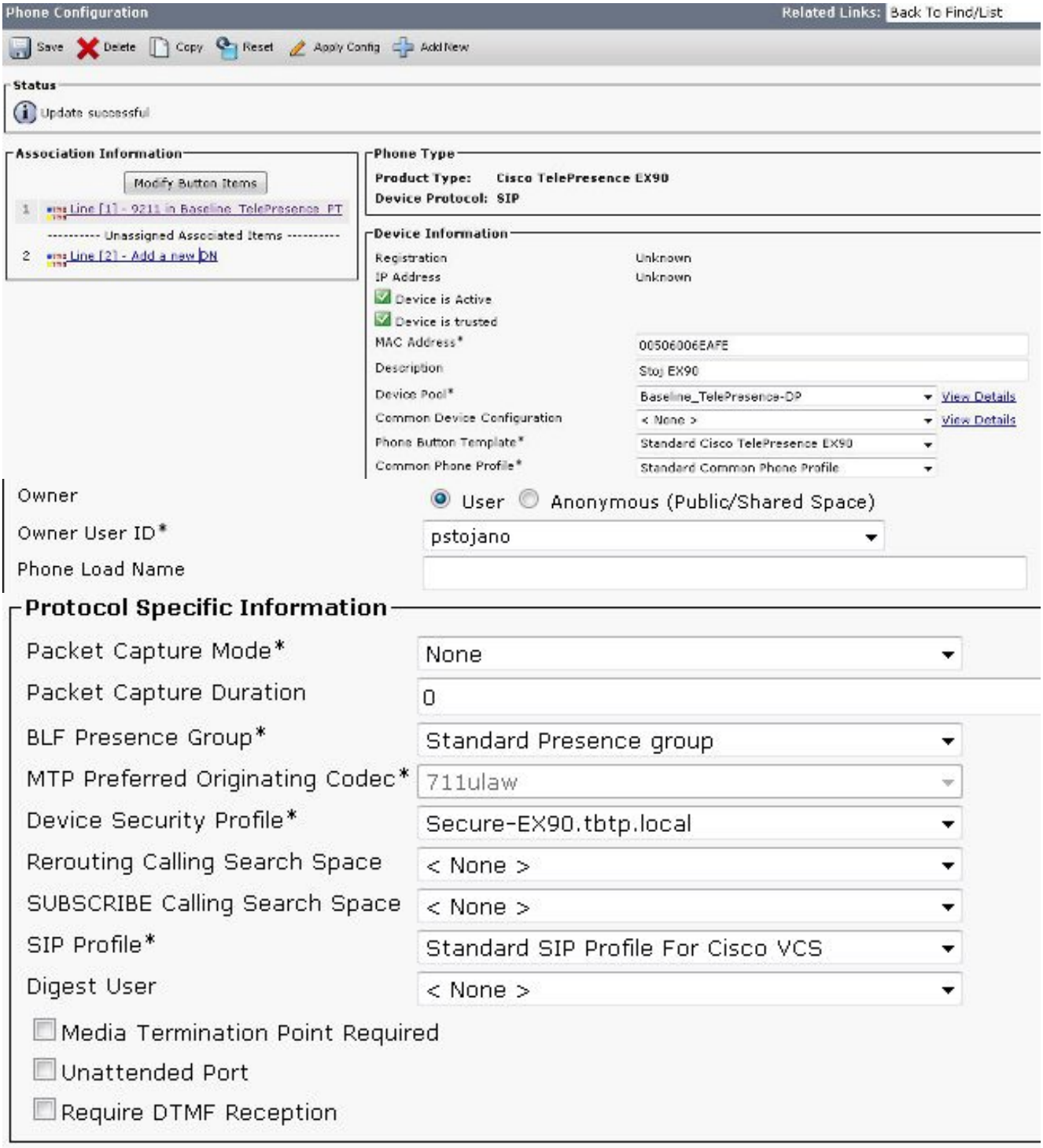
Guide de Sécurité CUCM 9.1(2)

Guide de Sécurité CUCM 10

Créez un profil dans CUCM pour le point final basé sur comité

1. Dans CUCM, **Device > Phone** choisi.

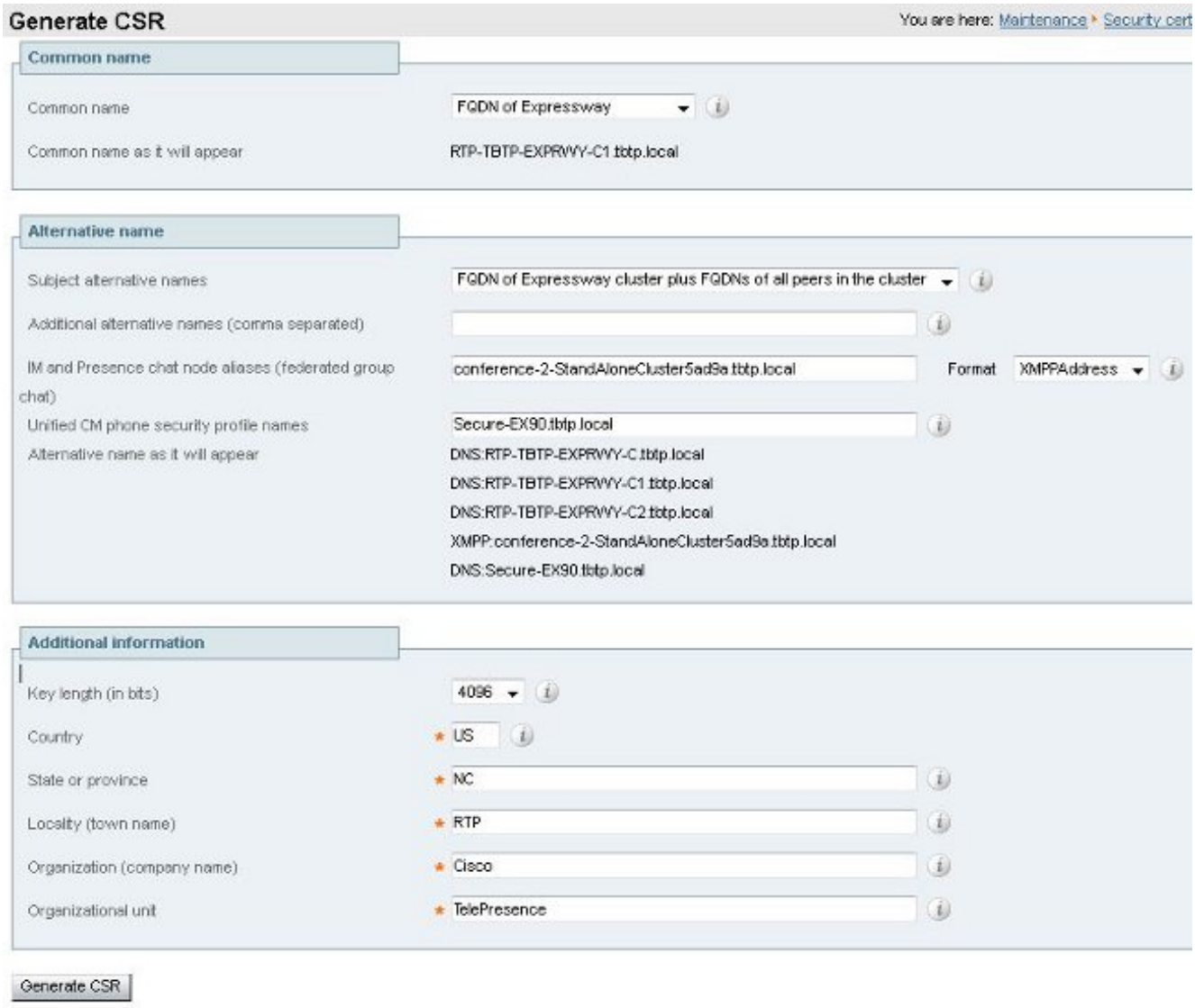
2. Cliquez sur Add **nouveau**.
3. Sélectionnez le type basé sur comité de point final et configurez ces paramètres : Adresse MAC - Adresse MAC du périphérique basé sur comitéChamps tenus le premier rôle exigés (*)Propriétaire - UtilisateurUser-id de propriétaire - Propriétaire associé avec le périphériqueProfil de sécurité des périphériques - Profil précédemment configuré (Secure-EX90.tbtp.local)Profil de SIP - Profil standard de SIP ou tout profil fait sur commande précédemment
créé



Ajoutez le nom de profil de Sécurité au SAN du certificat Expressway-C/VCS-C (facultatif)

1. Dans Expressway-C/VCS-C, la **maintenance** choisie **> la Sécurité délivre un certificat >**

certificat de serveur.
2. Le clic **génèrent le CSR**.
3. Complétez les champs de la demande de signature de certificat (CSR) et assurez-vous que « le nom de profil de degré de sécurité de téléphone d'Unified CM » a le profil précis de degré de sécurité de téléphone répertorié dans le format du nom de domaine complet (FQDN). Par exemple, Secure-EX90.tbtp.local.Remarque: Les noms de profil de degré de sécurité de téléphone d'Unified CM sont répertoriés au fond du champ soumis du nom secondaire (SAN).
4. Envoyez le CSR à un Autorité de certification (CA) de tiers interne ou à signer.
5. **La maintenance > la Sécurité** choisies **délivre un certificat > certificat de serveur** afin de télécharger le certificat à l'Expressway-C/VCS-C.

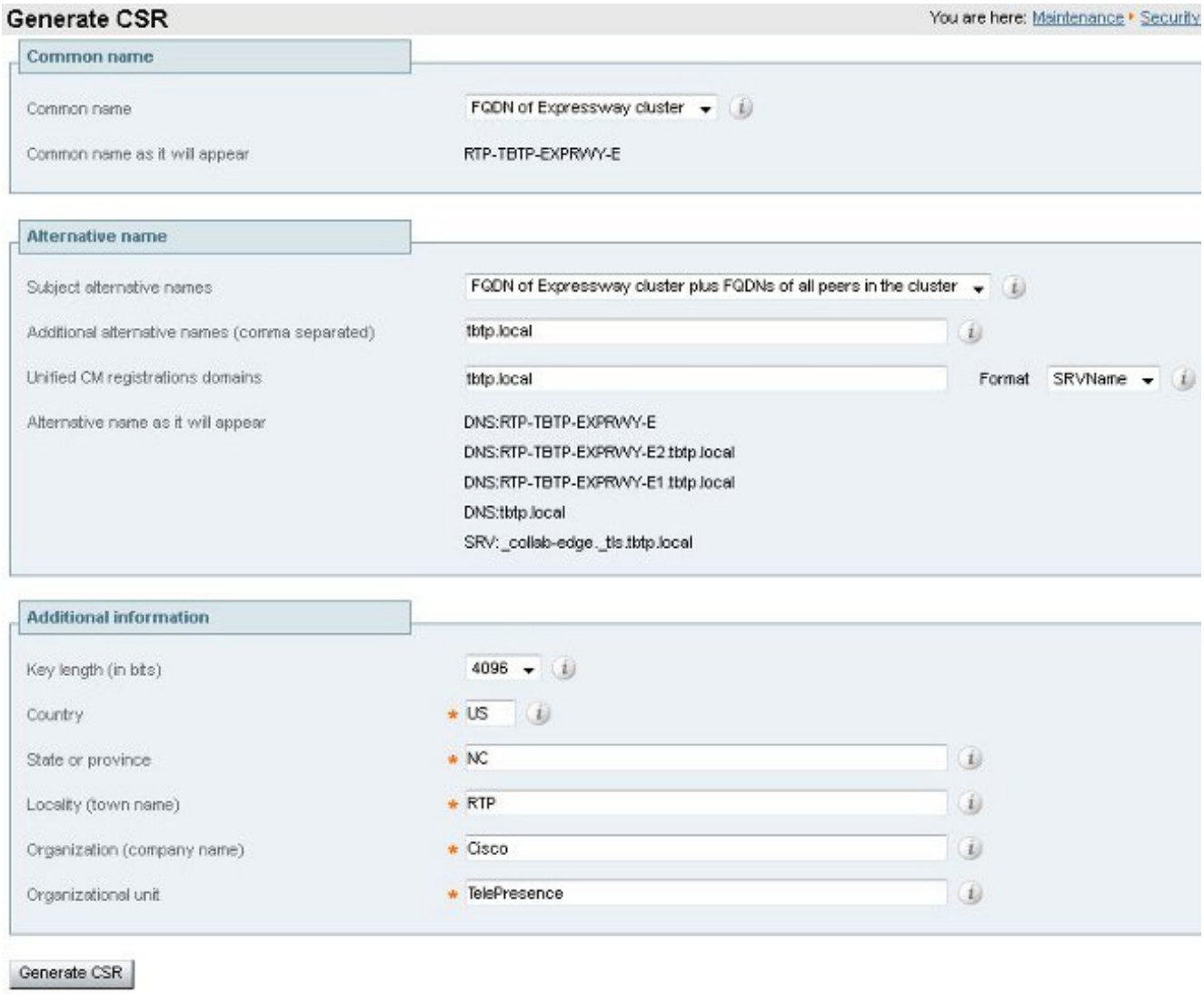


Ajoutez le domaine UC au certificat Expressway-E/VCS-E

1. Dans Expressway-E/VCS-E, la **maintenance** choisie **> la Sécurité délivre un certificat > certificat de serveur**.
2. Le clic **génèrent le CSR**.
3. Complétez les champs CSR et assurez-vous que « les domaines d'enregistrements d'Unified CM » contiennent le domaine au lequel le point final basé sur comité fera des demandes de périphérie de Collaboration (collab-périphérie), dans les formats de Domain Name Server

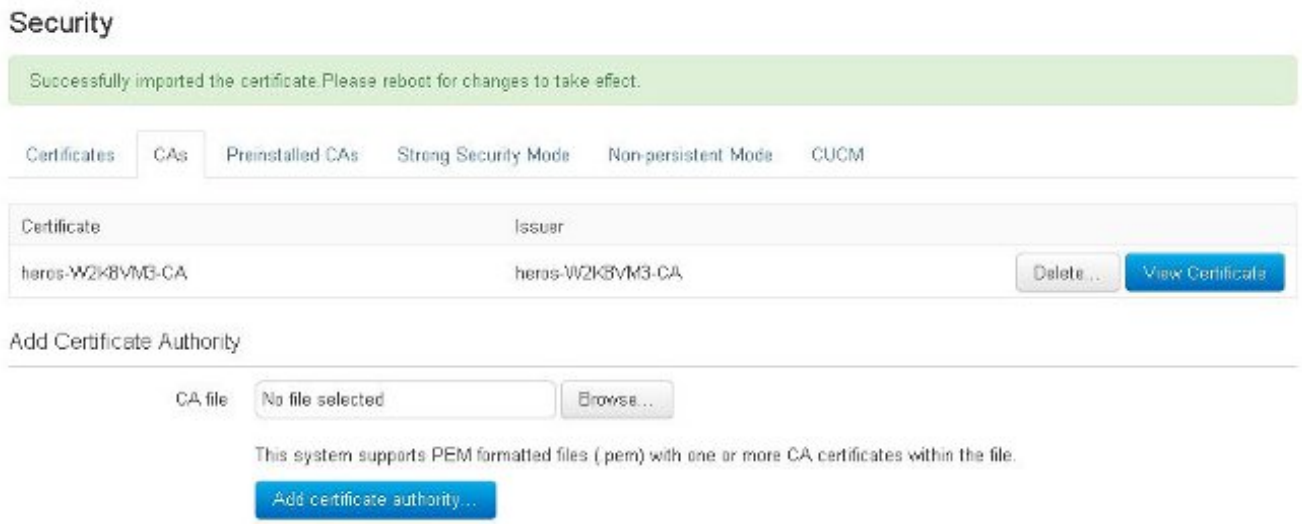
(DN) ou de nom de service (SRV).

4. Envoyez le CSR à un tiers interne ou CA à signer.
5. **La maintenance > la Sécurité** choisies **délivre un certificat > certificat de serveur** afin de télécharger le certificat à l'Expressway-E/VCS-E.

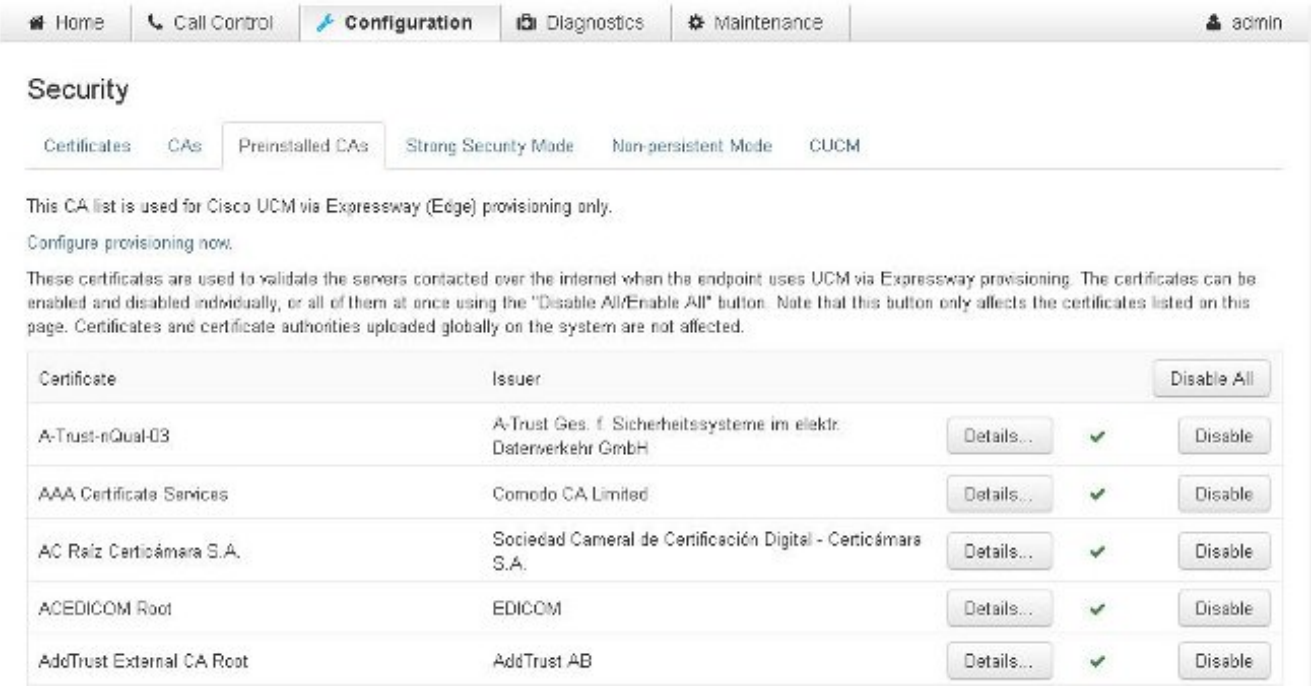


Installez le certificat de CA de confiance approprié sur le point final basé sur comité

1. Dans le point final basé sur comité, **configuration > Sécurité** choisies.
2. Sélectionnez l'onglet **CA** et recherchez le certificat de CA qui a signé votre certificat Expressway-E/VCS-E.
3. Cliquez sur Add l'**autorité de certification**.Remarque: Une fois le certificat t'est avec succès ajouté verra qu'il l'a répertorié dans la liste de certificat.



Remarque: Le comité technique 7.2 contient une liste préinstallée CAs. Si le CA qui a signé le certificat d'autoroute-e est contenu dans cette liste, les étapes répertoriées dans cette section ne sont pas
exigées.

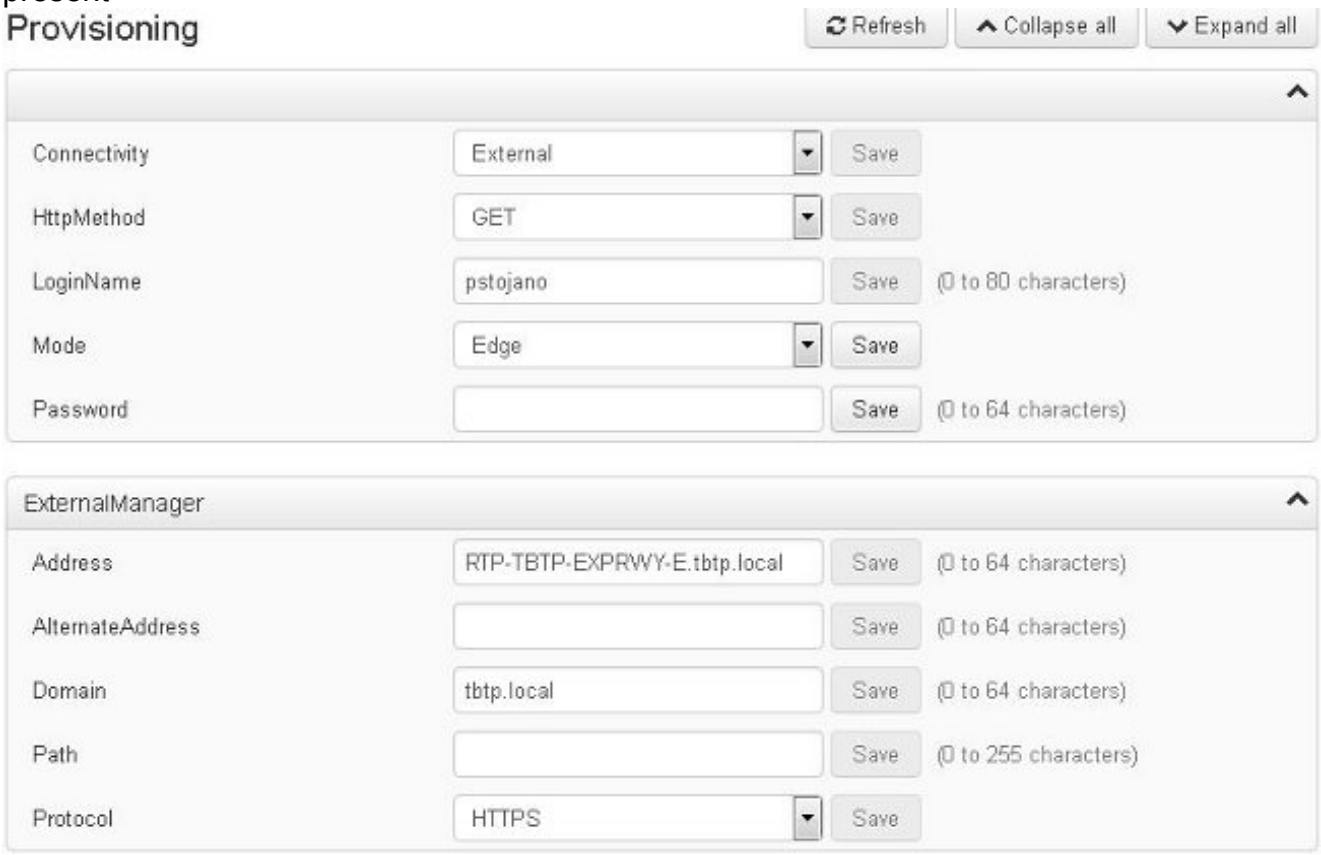


Remarque: La page préinstallée CAs contient un commode « configurent le ravitaillement maintenant » se boutonnent que vous porte directement à la configuration requise remarquable dans l'étape 2 dans la section suivante.

Installez un point final basé sur comité pour le ravitaillement de périphérie

1. Dans le point final basé sur comité, la **configuration > le réseau** choisis et s'assurent que ces champs sont correctement complétés sous la section de DN : le nom de domaineAdresse du serveur
2. Dans le point final basé sur comité, la **configuration > le ravitaillement** choisis et s'assurent que ces champs sont correctement complétés : LoginName - comme défini dans CUCMMode - **Périphérie**Mot de passe - comme défini dans CUCM
Gestionnaire externeAdresse - Adresse Internet de votre Expressway-E/VCS-EDomaine -

Domaine où votre enregistrement de collab-périphérie est présent



Vérifiez

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

point final basé sur comité

1. Dans le GUI de Web, naviguez « à la maison ». Recherchez la 'section du proxy SIP 1" pour un état « enregistré ». L'adresse de proxy est votre Expressway-E/VCS-E.

2. Du CLI, entrez dans le **xstatus //prov**. Si vous êtes enregistré vous devriez voir un état de ravitaillement de « Provisioned ». **xstatus //prov**

```
*s Network 1 IPv4 DHCP ProvisioningDomain: ""
*s Network 1 IPv4 DHCP ProvisioningServer: ""
*s Provisioning CUCM CAPF LSC: Installed
*s Provisioning CUCM CAPF Mode: IgnoreAuth
```

```
*s Provisioning CUCM CAPF OperationResult: NotSet
*s Provisioning CUCM CAPF OperationState: NonPending
*s Provisioning CUCM CAPF ServerName: ""
*s Provisioning CUCM CAPF ServerPort: 0
*s Provisioning CUCM CTL State: Installed
*s Provisioning CUCM ExtensionMobility Enabled: False
*s Provisioning CUCM ExtensionMobility LastLoggedInUserId: ""
*s Provisioning CUCM ExtensionMobility LoggedIn: False
*s Provisioning CUCM ITL State: Installed
*s Provisioning CUCM ProvisionSecurity: Signed
*s Provisioning CUCM TVS Proxy 1 IPv6Address: ""
*s Provisioning CUCM TVS Proxy 1 Port: 2445
*s Provisioning CUCM TVS Proxy 1 Priority: 0
*s Provisioning CUCM TVS Proxy 1 Server: "xx.xx.97.131"
*s Provisioning CUCM UserId: "pstojano"
*s Provisioning NextRetry: ""
*s Provisioning Reason: ""
*s Provisioning Server: "xx.xx.97.131"
*s Provisioning Software Current CompletedAt: ""
*s Provisioning Software Current URL: ""
*s Provisioning Software Current VersionId: ""
*s Provisioning Software UpgradeStatus LastChange: "2014-06-30T19:08:40Z"
*s Provisioning Software UpgradeStatus Message: ""
*s Provisioning Software UpgradeStatus Phase: None
*s Provisioning Software UpgradeStatus SecondsUntilUpgrade: 0
*s Provisioning Software UpgradeStatus SessionId: ""
*s Provisioning Software UpgradeStatus Status: None
*s Provisioning Software UpgradeStatus URL: ""
*s Provisioning Software UpgradeStatus VersionId: ""
*s Provisioning Status: Provisioned
** end
```

CUCM

Dans CUCM, **Device > Phone** choisi. Parcourez la liste ou filtrez la liste en fonction sur votre point final. Vous devriez voir « inscrit à un message de %CUCM_IP% ». L'adresse IP à la droite de ceci devrait être votre Expressway-C/VCS-C qui des proxys l'enregistrement.

Autoroute-C

1. Dans Expressway-C/VCS-C, l'**état** choisi **> a unifié des transmissions > des sessions de ravitaillement de vue.**
2. Filtrez par l'adresse IP de votre point final basé sur comité. Un exemple d'une session Provisioned est affiché ici
:

Dépannez

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

Les questions d'enregistrement mettent en boîte sont provoqué par par les nombreux facteurs qui

incluent des DN, des questions de certificat, configuration, et ainsi de suite. Cette section inclut une liste complète de ce que vous verriez typiquement si vous rencontrez un problème donné et de comment au remediate il. Si vous vous exécutez dans des questions en dehors de ce qui a été déjà documenté, sentez-vous libre de l'inclure.

Outils

Pour commencer, rendez-vous compte des outils à votre disposition.

Point final comité technique

GUI Web

- all.log
- Se connecter étendu par début (incluez une pleine capture de paquet)

CLI

Ces commandes sont les plus salutaires afin de dépanner en temps réel :

- le ctx HttpClient de log mettent au point 9
- le ctx PROV de log mettent au point 9
- log sorti sur <-- Expositions se connectant par l'intermédiaire de la console

Une façon efficace de recréer le problème est de basculer le mode de ravitaillement de la « périphérie » à "OFF" et puis de nouveau à la « périphérie » dans le GUI de Web. Vous pouvez également entrer le **mode de ravitaillement de xConfiguration :** commande dans le CLI.

Autoroutes

- Logs diagnostiques
- TCPDump

CUCM

- Suivis SDI/SDL

Question 1 : l'enregistrement de Collab-périphérie n'est pas visible et/ou l'adresse Internet n'est pas résoluble

Comme vous pouvez voir, le get_edge_config échoue en raison de la résolution de noms.

Logs de point final comité technique

```
15716.23 HttpClient   HTTPClientCurl error
(https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/):
'Couldn't resolve host name'

15716.23 PROV ProvisionRequest failed: 4 (Couldn't resolve host name)
```

```
15716.23 PROV I: notify_http_done: Received 0 (Couldn't resolve host name) on request
https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/
```

Correction

1. Vérifiez si l'enregistrement de collab-périphérie est présent et renvoie l'adresse Internet correcte.
2. Vérifiez si les informations de serveur de DNS configurées sur le client sont correctes.

Issue 2 : Le CA n'est pas présent dans la liste de confiance CA sur le point final basé sur comité

Logs de point final comité technique

```
15975.85 HttpClient     Trying xx.xx.105.108...
15975.85 HttpClient Adding handle: conn: 0x48390808
15975.85 HttpClient Adding handle: send: 0
15975.86 HttpClient Adding handle: recv: 0
15975.86 HttpClient Curl_addHandleToPipeline: length: 1
15975.86 HttpClient - Conn 64 (0x48396560) send_pipe: 0, recv_pipe: 0
15975.87 HttpClient - Conn 65 (0x4835a948) send_pipe: 0, recv_pipe: 0
15975.87 HttpClient - Conn 67 (0x48390808) send_pipe: 1, recv_pipe: 0
15975.87 HttpClient Connected to RTP-TBTP-EXPRWY-E.tbtp.local (xx.xx.105.108)
port 8443 (#67)
15975.87 HttpClient successfully set certificate verify locations:
15975.87 HttpClient CAfile: none
CApath: /config/certs/edge_ca_list
15975.88 HttpClient Configuring ssl context with special Edge certificate verifier
15975.88 HttpClient SSLv3, TLS handshake, Client hello (1):
15975.88 HttpClient SSLv3, TLS handshake, Server hello (2):
15975.89 HttpClient SSLv3, TLS handshake, CERT (11):
15975.89 HttpClient SSLv3, TLS alert, Server hello (2):
15975.89 HttpClient SSL certificate problem: self signed certificate in
certificate chain
15975.89 HttpClient Closing connection 67
15975.90 HttpClient HTTPClientCurl error
(https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/):
'Peer certificate cannot be authenticated with given CA certificates'

15975.90 PROV ProvisionRequest failed: 4 (Peer certificate cannot be
authenticated with given CA certificates)
15975.90 PROV I: notify_http_done: Received 0 (Peer certificate cannot be
authenticated with given CA certificates) on request
https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/
15975.90 PROV EDGEProvisionUser: start retry timer for 15 seconds
```

Correction

1. Vérifiez si un tiers CA est répertorié sous l'onglet de **Sécurité > CAs** sur le point final.
2. Si le CA est répertorié, vérifiez qu'il est correct.

Question 3 : L'autoroute-e n'a pas le domaine UC répertorié dans le SAN

Logs de point final comité technique

```
82850.02 CertificateVerification ERROR: [verify_edge_domain_in_san]: Edge TLS
verification failed: Edge domain 'tbtp.local' and corresponding SRVName
'_collab-edge._tls.tbtp.local' not found in certificate SAN list
82850.02 HttpClient SSLv3, TLS alert, Server hello (2):
```

```
82850.02 HttpClient SSL certificate problem: application verification failure
82850.02 HttpClient Closing connection 113
82850.02 HttpClient HTTPClientCurl error
(https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/):
'Peer certificate cannot be authenticated with given CA certificates'
```

Autoroute-e SAN

```
X509v3 Subject Alternative Name:
DNS:RTP-TBTP-EXPRWY-E.tbtp.local, SRV:_collab-edge._tls.tbtppppp.local
```

Correction

1. CSR régénéré d'autoroute-e afin d'inclure les domaines UC.
2. Il est possible que sur le point final comité technique le paramètre « de domaine d'ExternalManager » ne soit pas placé à ce qu'est le domaine UC. Si c'est le cas vous devez l'apparier.

Question 4 : Le nom d'utilisateur et/ou le mot de passe fournis dans le profil de ravitaillement comité technique est incorrect

Logs de point final comité technique

```
83716.67 HttpClient     Server auth using Basic with user 'pstojano'
83716.67 HttpClient GET /dGJ0cC5jb20/get_edge_config/ HTTP/1.1
Authorization: xxxxxx
Host: RTP-TBTP-EXPRWY-E.tbtp.local:8443
Cookie: JSESSIONIDSSO=34AFA4A6DEE1DDCE8B1D2694082A6D0A
Content-Type: application/x-www-form-urlencoded
Accept: text/xml
User-Agent: Cisco/TC
Accept-Charset: ISO-8859-1,utf-8
83716.89 HttpClient HTTP/1.1 401 Unauthorized
83716.89 HttpClient Authentication problem. Ignoring this.
83716.90 HttpClient WWW-Authenticate: Basic realm="Cisco-Edge"
83716.90 HttpClient Server CE_C ECS is not blacklisted
83716.90 HttpClient Server: CE_C ECS
83716.90 HttpClient Date: Thu, 25 Sep 2014 17:42:51 GMT
83716.90 HttpClient Age: 0
83716.90 HttpClient Transfer-Encoding: chunked
83716.91 HttpClient Connection: keep-alive
83716.91 HttpClient
83716.91 HttpClient 0
83716.91 HttpClient Connection #116 to host RTP-TBTP-EXPRWY-E.tbtp.local
left intact
83716.91 HttpClient HTTPClientCurl received HTTP error 401

83716.91 PROV ProvisionRequest failed: 5 (HTTP code=401)
83716.91 PROV I: notify_http_done: Received 401 (HTTP code=401) on request
https://RTP-TBTP-EXPRWY-E.tbtp.local:8443/dGJ0cC5jb20/get_edge_config/
```

Expressway-C/VCS-C

```
2014-09-25T13:46:20-04:00 RTP-TBTP-EXPRWY-C edgeconfigprovisioning
UTCTime="2014-09-25 17:46:20,92" Module="network.http.edgeconfigprovisioning"
Level="DEBUG" Action="Received"
Request-url="https://xx.xx.97.131:8443/cucm-uds/user/pstojano/devices"
HTTPMSG:
|HTTP/1.1 401 Unauthorized
Expires: Wed, 31 Dec 1969 19:00:00 EST
Server:
Cache-Control: private
```

```
Date: Thu, 25 Sep 2014 17:46:20 GMT
Content-Type: text/html;charset=utf-8
WWW-Authenticate: Basic realm="Cisco Web Services Realm"

2014-09-25T13:46:20-04:00 RTP-TBTP-EXPRWY-C UTCTime="2014-09-25 17:46:20,92"
Module="developer.edgeconfigprovisioning.server" Level="DEBUG"
CodeLocation="edgeprotocol(1018)" Detail="Failed to authenticate user against server"
Username="pstojano" Server="('https', 'xx.xx.97.131', 8443)"
Reason="<twisted.python.failure.Failure <type 'exceptions.Exception'>>
"2014-09-25T13:46:20-04:00 RTP-TBTP-EXPRWY-C edgeconfigprovisioning:
Level="INFO" Detail="Failed to authenticate user against server" Username="pstojano"
Server="('https', 'xx.xx.97.131', 8443)" Reason="<twisted.python.failure.Failure
<type 'exceptions.Exception'>>" UTCTime="2014-09-25 17:46:20,92"
```

Correction

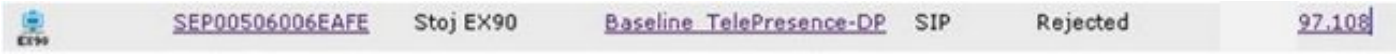
1. Vérifiez que le nom d'utilisateur/mot de passe entré sous la page de ravitaillement sur le point final comité technique est valide.
2. Vérifiez les qualifications contre la base de données CUCM. Version 10 - utilisez le portail de self careVersion 9 - utilisez les options utilisateur cm

L'URL pour les deux portails est identique : https://%CUCM%/ucmuser/

Si présenté avec une erreur insuffisante de droites, assurez que ces rôles sont assignés à l'utilisateur :

- CTI standard activé
- Utilisateur final de la norme CCM

Question 5 : L'enregistrement basé sur comité de point final obtient rejeté



Suivis CUCM

```
08080021.043 |16:31:15.937 |AppInfo  |SIPStationD(18400) - validTLSConnection:TLS
InvalidX509NameInCertificate, Rcvd=RTP-TBTP-EXPRWY-C.tbtp.local,
Expected=SEP00506006EAFE. Will check SAN the next
08080021.044 |16:31:15.937 |AppInfo |SIPStationD(18400) - validTLSConnection:TLS
InvalidX509NameInCertificate Error , did not find matching SAN either,
Rcvd=RTP-TBTP-EXPRWY-C.tbtp.local, Expected=Secure-EX90.tbtp.local
08080021.045 |16:31:15.937 |AppInfo |ConnectionFailure - Unified CM failed to open
a TLS connection for the indicated device Device Name:SEP00506006EAFE
IP Address:xx.xx.97.108 IPV6Address: Device type:584 Reason code:2 App ID:Cisco
CallManager Cluster ID:StandAloneCluster Node ID:RTP-TBTP-CUCM9 08080021.046
|16:31:15.938 |AlarmErr |AlarmClass: CallManager, AlarmName: ConnectionFailure,
AlarmSeverity: Error, AlarmMessage: , AlarmDescription: Unified CM failed to open
a TLS connection for the indicated device, AlarmParameters:
DeviceName:SEP00506006EAFE, IPAddress:xx.xx.97.108, IPV6Address:,
DeviceType:584, Reason:2, AppID:Cisco CallManager, ClusterID:StandAloneCluster,
NodeID:RTP-TBTP-CUCM9,
```

Point final comité technique

Effectif Expressway-C/VCS-C

```
08080021.043 |16:31:15.937 |AppInfo  |SIPStationD(18400) - validTLSConnection:TLS
InvalidX509NameInCertificate, Rcvd=RTP-TBTP-EXPRWY-C.tbtp.local,
Expected=SEP00506006EAFE. Will check SAN the next
08080021.044 |16:31:15.937 |AppInfo |SIPStationD(18400) - validTLSConnection:TLS
InvalidX509NameInCertificate Error , did not find matching SAN either,
Rcvd=RTP-TBTP-EXPRWY-C.tbtp.local, Expected=Secure-EX90.tbtp.local
08080021.045 |16:31:15.937 |AppInfo |ConnectionFailure - Unified CM failed to open
a TLS connection for the indicated device Device Name:SEP00506006EAFE
IP Address:xx.xx.97.108 IPV6Address: Device type:584 Reason code:2 App ID:Cisco
CallManager Cluster ID:StandAloneCluster Node ID:RTP-TBTP-CUCM9 08080021.046
|16:31:15.938 |AlarmErr |AlarmClass: CallManager, AlarmName: ConnectionFailure,
AlarmSeverity: Error, AlarmMessage: , AlarmDescription: Unified CM failed to open
a TLS connection for the indicated device, AlarmParameters:
DeviceName:SEP00506006EAFE, IPAddress:xx.xx.97.108, IPV6Address:,
DeviceType:584, Reason:2, AppID:Cisco CallManager, ClusterID:StandAloneCluster,
NodeID:RTP-TBTP-CUCM9,
```

Dans cet exemple spécifique de log il est clair que l'Expressway-C/VCS-C ne contienne pas le FQDN de profil de degré de sécurité de téléphone dans le SAN. (Secure-EX90.tbtp.local). Dans la prise de contact de Transport Layer Security (TLS), le CUCM examine le certificat de serveur Expressway-C/VCS-C. Puisqu'il ne le trouve pas dans le SAN il jette l'erreur bolded et des signaler qu'il a attendu le profil de degré de sécurité de téléphone dans le format FQDN.

Correction

1. Vérifiez que l'Expressway-C/VCS-C contient le profil de degré de sécurité de téléphone dans le format FQDN dans le SAN de lui est certificat de serveur.
2. Vérifiez que le périphérique utilise le profil de Sécurité correct dans CUCM si vous utilisez un profil sécurisé dans le format FQDN.
3. Ceci pourrait sont provoqué par également par l'ID de bogue Cisco CSCuq86376. Si c'est le contrôle de cas la taille Expressway-C/VCS-C SAN et la position du profil de degré de sécurité de téléphone dans le SAN.

Informations connexes

- Mobile et guide d'Accès à distance
- Guide de création de certificat VCS
- EX90/EX60 obtenant le guide de démarrage
- Guide de l'administrateur CUCM 9.1
- Support et documentation techniques - Cisco Systems