Exemple de configuration de terminaux basés sur TC de la périphérie de collaboration

Contenu

Introduction

Le document décrit ce qui est nécessaire pour configurer et dépanner l'enregistrement des terminaux basés sur TelePresence Codec (TC) via la solution Mobile and Remote Access.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Solution d'accès mobile et à distance
- Certificats VCS (Video Communication Server)
- Expressway X8.1.1 ou version ultérieure
- Cisco Unified Communication Manager (CUCM) version 9.1.2 ou ultérieure
- Terminaux basés sur TC
- CE8.x nécessite la clé d'option de cryptage pour activer « Edge » en tant qu'option de provisionnement

Components Used

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

- VCS X8.1.1 ou version ultérieure
- CUCM version 9.1(2)SU1 ou ultérieure et IM & Presence version 9.1(1) ou ultérieure
- Microprogramme TC 7.1 ou ultérieur **(TC7.2 recommandé)**
- Contrôle et Expressway/Expressway Core et Edge VCS
- CUCM
- Point de terminaison TC

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. If your network is live, make sure that you understand the potential impact of any command.

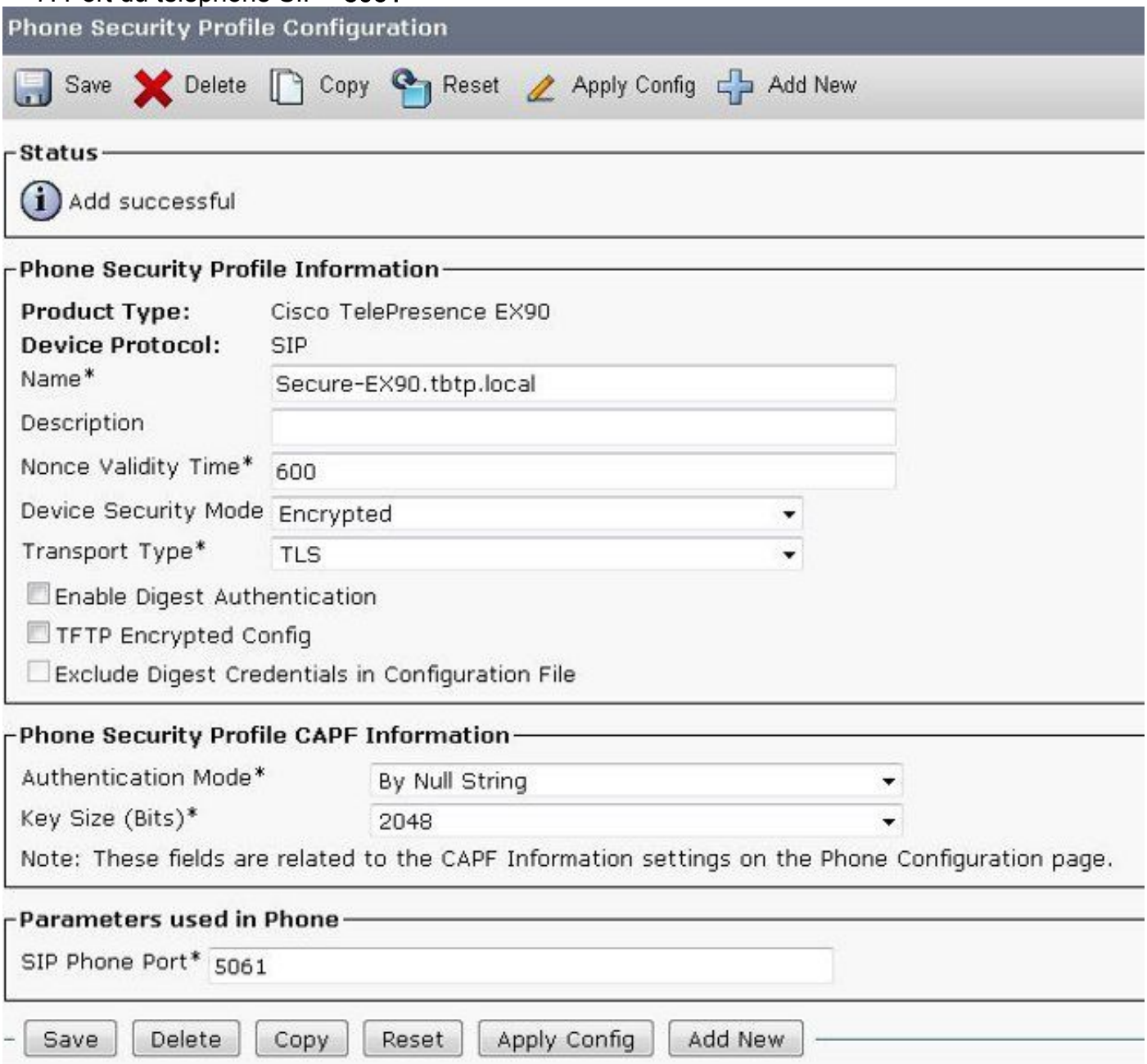
Configuration

Ces étapes de configuration supposent que l'administrateur va configurer le point de terminaison basé sur TC pour l'enregistrement sécurisé des périphériques. L'enregistrement sécurisé n'est

PAS obligatoire, mais le guide de solution Mobile and Remote Access donne l'impression que c'est parce qu'il y a des captures d'écran de la configuration qui montrent des profils de périphériques sécurisés sur CUCM.

Étape 1. Créez un profil de téléphone sécurisé sur CUCM au format FQDN (facultatif).

1. Dans CUCM, sélectionnez **System > Security > Phone Security Profile**.
2. Cliquez sur **Ajouter nouveau**.
3. Sélectionnez le type de point de terminaison basé sur TC et configurez les paramètres suivants :
4. Nom - **Secure-EX90.tbtp.local (format FQDN requis)**
5. Mode de sécurité du périphérique - **crypté**
6. Type de transport - **TLS**
7. Port du téléphone SIP - **5061**



Étape 2. Assurez-vous que le mode de sécurité du cluster est (1) - Mixte (facultatif).

1. Dans CUCM, sélectionnez **System > Enterprise Parameters**.
2. Faites défiler jusqu'à **Paramètres de sécurité > Mode de sécurité du cluster > 1**.

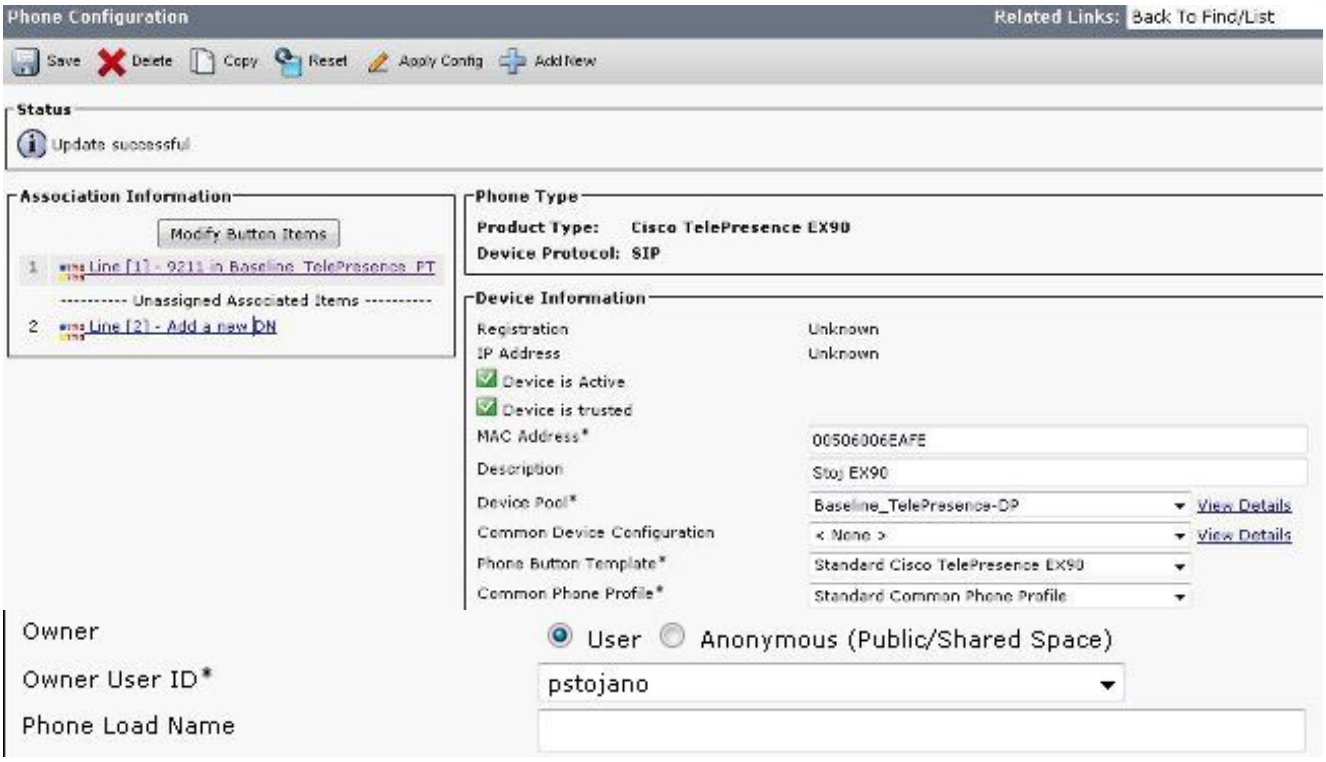
Si la valeur n'est pas 1, CUCM n'a pas été sécurisé. Si tel est le cas, l'administrateur doit examiner l'un de ces deux documents afin de sécuriser CUCM.

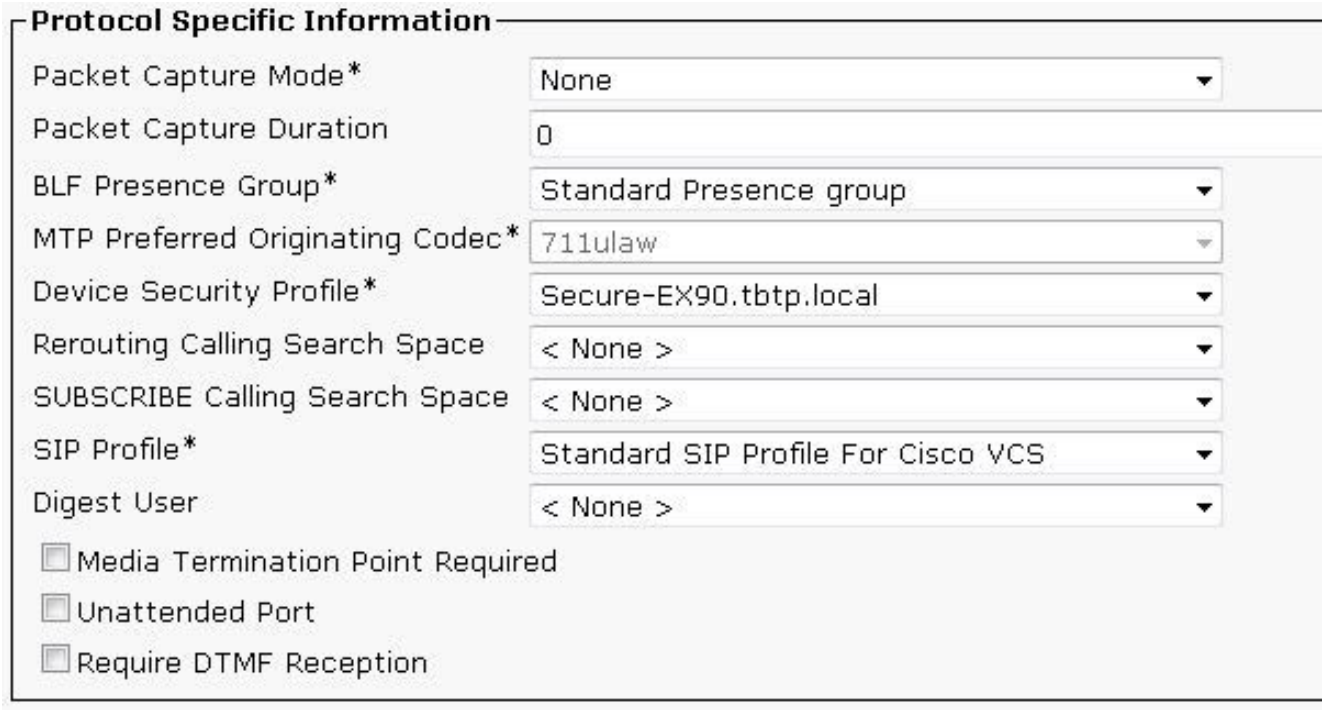
Guide de sécurité CUCM 9.1(2)

Guide de sécurité CUCM 10

Étape 3. Créez un profil dans CUCM pour le point de terminaison basé sur TC.

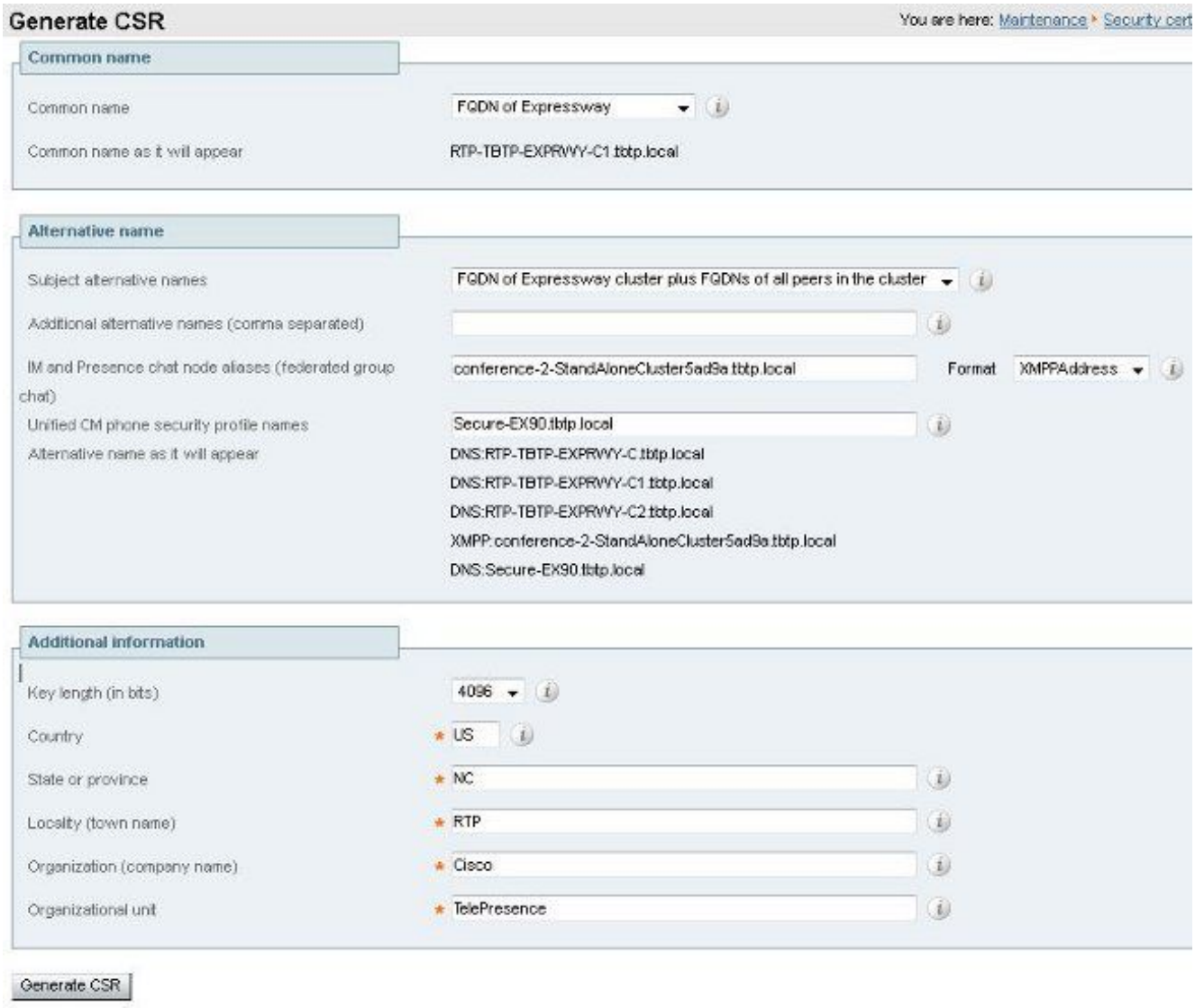
1. Dans CUCM, sélectionnez **Device > Phone**.
2. Cliquez sur **Ajouter nouveau**.
3. Sélectionnez le type de point de terminaison basé sur TC et configurez les paramètres suivants : Adresse MAC : adresse MAC du périphérique basé sur TCChamps étoilés obligatoires (*)Propriétaire - UtilisateurID utilisateur propriétaire - Propriétaire associé au périphériqueProfil de sécurité des périphériques - Profil précédemment configuré (Secure-EX90.tbtp.local)Profil SIP - Profil SIP standard ou tout profil personnalisé précédemment créé





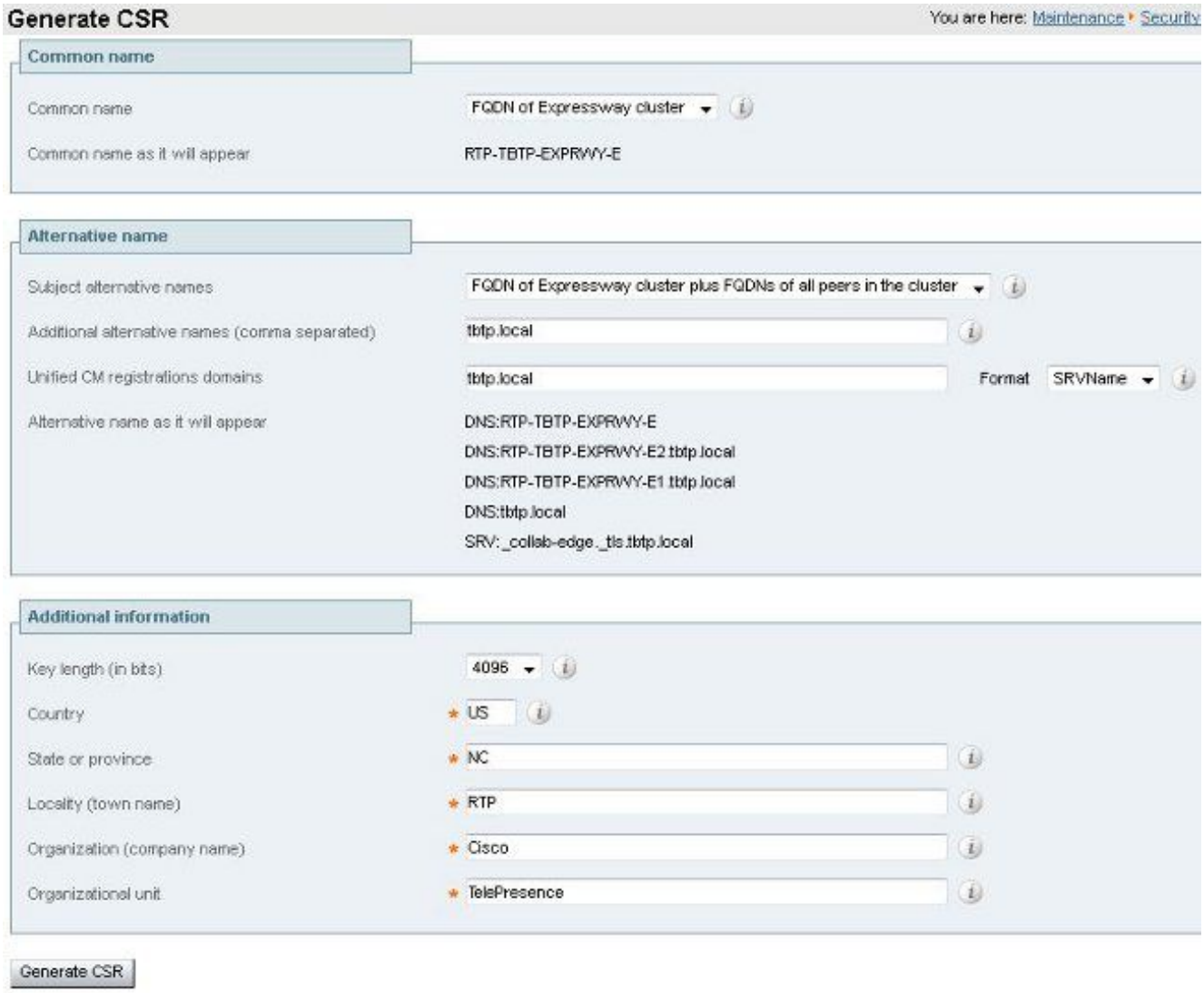
Étape 4. Ajoutez le nom du profil de sécurité au SAN du certificat Expressway-C/VCS-C (facultatif).

1. Dans Expressway-C/VCS-C, accédez à **Maintenance > Security Certificates > Server Certificate**.
2. Cliquez sur **Generate CSR**.
3. Complétez les champs de demande de signature de certificat (CSR) et assurez-vous que le **nom du profil de sécurité du téléphone Unified CM** a le profil de sécurité du téléphone indiqué au format FQDN (Fully Qualified Domain Name). Par exemple, **Secure-EX90.tbtp.local**. **Note**: Les noms des profils de sécurité du téléphone Unified CM sont répertoriés à l'arrière du champ Subject Alternate Name (SAN).
4. Envoyez le CSR à une autorité de certification interne ou tierce à signer.
5. Sélectionnez **Maintenance > Security Certificates > Server Certificate** afin de télécharger le certificat sur Expressway-C/VCS-C.



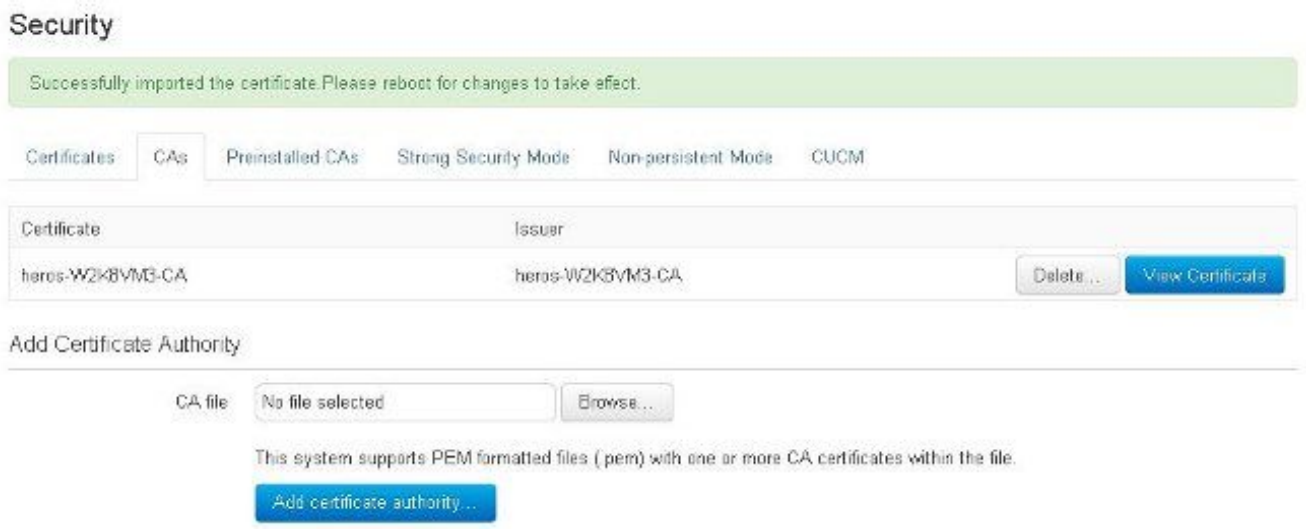
Étape 5. Ajoutez le domaine UC au certificat Expressway-E/VCS-E.

1. Dans Expressway-E/VCS-E, sélectionnez **Maintenance > Certificats de sécurité > Certificat de serveur**.
2. Cliquez sur **Generate CSR**.
3. Complétez les champs CSR et assurez-vous que les domaines d'enregistrement Unified CM contiennent le domaine auquel le point de terminaison basé sur TC effectuera des demandes Collaboration Edge (collab-edge), soit au format DNS (Domain Name Server), soit au format SRV (Service Name Name Server).
4. Envoyez le CSR à une CA interne ou tierce pour signature.
5. Sélectionnez **Maintenance > Security Certificates > Server Certificate** afin de télécharger le certificat sur l'Expressway-E/VCS-E.

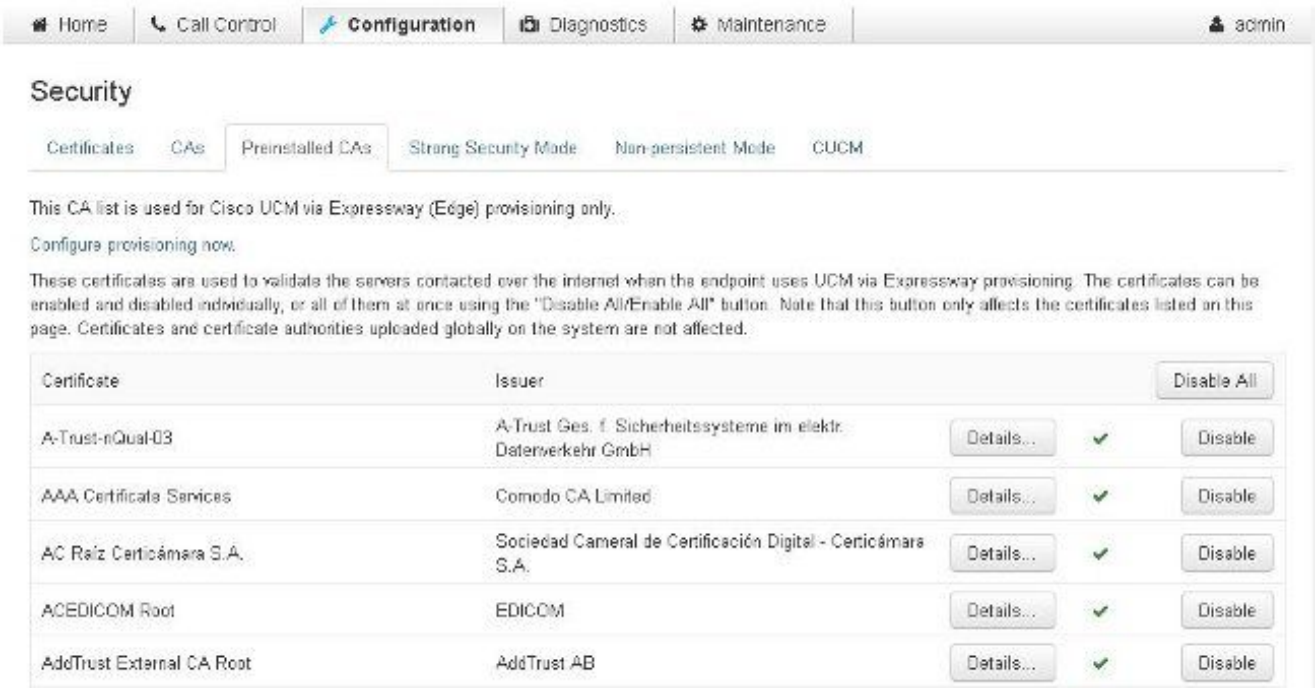


Étape 6. Installez le certificat CA de confiance approprié sur le point de terminaison basé sur TC.

1. Dans le point de terminaison basé sur TC, sélectionnez **Configuration > Security**.
2. Sélectionnez l'onglet **CA** et recherchez le certificat CA qui a signé votre certificat Expressway-E/VCS-E.
3. Cliquez sur **Ajouter une autorité de certificat**. **Note**: Une fois le certificat ajouté, il apparaît dans la liste
   Certificats.



Note: TC 7.2 contient une liste d'AC préinstallée. Si l'autorité de certification ayant signé le certificat Expressway-E figure dans cette liste, les étapes répertoriées dans cette section ne sont pas
obligatoires.

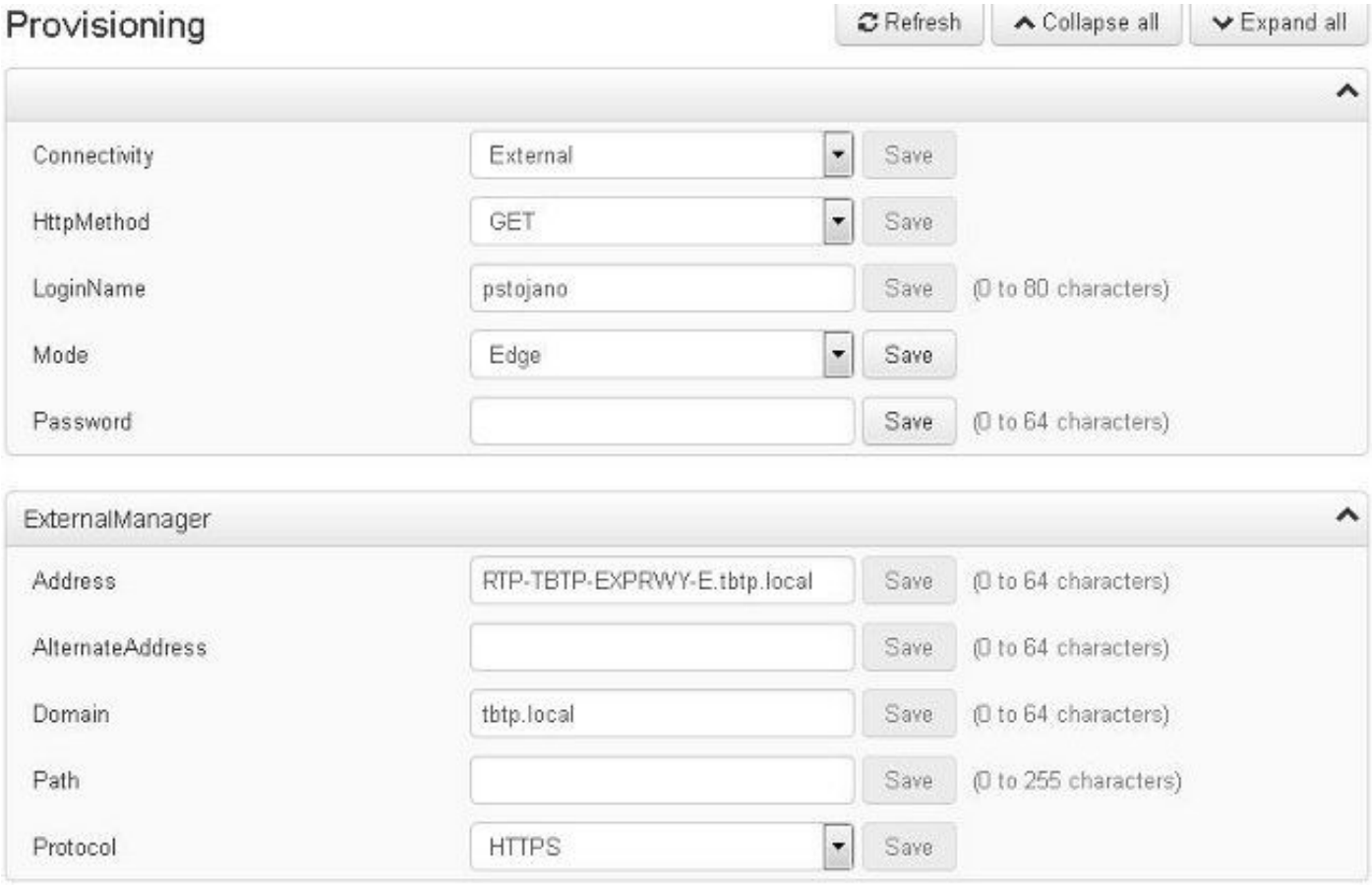


Note: La page CA préinstallée contient un bouton pratique « Configurer le provisionnement maintenant » qui vous amène directement à la configuration requise indiquée à l'étape 2 de la section suivante.

Étape 7. Configuration d'un point de terminaison basé sur TC pour le provisionnement Edge

- Dans le point de terminaison basé sur TC, sélectionnez **Configuration > Network** et assurez-vous que ces champs sont correctement renseignés sous la section DNS :
  le nom de domaine
  Adresse du serveur

- Dans le point de terminaison basé sur TC, sélectionnez **Configuration > Provisioning** et assurez-vous que ces champs sont correctement renseignés :
  Nom de connexion - tel que défini dans CUCM
  Mode - **Périphérie**
  Mot de passe - tel que défini dans CUCM
  Gestionnaire externe
  Adresse : nom d'hôte de votre Expressway-E/VCS-E
  Domaine - Domaine où se trouve votre enregistrement de périphérie de groupe



Vérification

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

Point de terminaison basé sur TC

1. Dans l'interface utilisateur graphique Web, accédez à Accueil. Recherchez la section 'SIP Proxy 1' pour un état « Registered ». L'adresse du proxy est votre Expressway-E/VCS-E.

2. Àpartir de l'interface de ligne de commande, saisissez **xstatus //provinces**. Si vous êtes inscrit, l'état Provisioning de « Provisioned » doit s'afficher.

```
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, sélectionnez **Device > Phone**. Faites défiler la liste ou filtrez la liste en fonction de votre point de terminaison. Vous devriez voir un message « Inscrit avec %CUCM_IP%« . L'adresse IP située à droite de cette page doit être votre Expressway-C/VCS-C qui effectue un proxy pour l'enregistrement.

Expressway-C

- Dans Expressway-C/VCS-C, sélectionnez **Status > Unified Communications > View Provisioning sessions.**
- Filtrer par l'adresse IP de votre point de terminaison basé sur TC. L'image illustre un exemple de session provisionnée :

Dépannage

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

Les problèmes d'enregistrement peuvent être causés par de nombreux facteurs, notamment le DNS, les problèmes de certificat, la configuration, etc. Cette section comprend une liste complète de ce que vous verriez généralement si vous rencontrez un problème donné et comment le

résoudre. Si vous rencontrez des problèmes en dehors de ce qui a déjà été documenté, n'hésitez pas à les inclure.

Outils

Pour commencer, soyez attentif aux outils à votre disposition.

Point de terminaison TC

GUI Web

- all.log
- Démarrer la journalisation étendue (inclure une capture de paquets complète)

CLI

Ces commandes sont les plus utiles pour le dépannage en temps réel :

- log ctx HttpClient debug 9
- log ctx PROV debug 9
- sortie du journal sur < : affiche la journalisation via la console

Pour recréer efficacement le problème, basculez le mode Provisioning de « Edge » à « Off », puis revenez à « Edge » dans l'interface utilisateur graphique Web. Vous pouvez également entrer le **mode d'approvisionnement xConfiguration :** dans la CLI.

Expressways

- Journaux de diagnostic
- TCPDump

CUCM

- Traces SDI/SDL

Problème 1: L'enregistrement de la périphérie de la baie de disques n'est pas visible et/ou le nom d'hôte n'est pas résoluble

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

Journaux des terminaux TC

```
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 collab-edge est présent et retourne le nom d'hôte correct.
2. Vérifiez si les informations du serveur DNS configurées sur le client sont correctes.

Problème 2: L'autorité de certification n'est pas présente dans la liste des autorités de certification de confiance sur le point de terminaison basé sur TC

Journaux des terminaux TC

```
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 une CA tierce est répertoriée sous l'onglet **Security > CAs** du point de terminaison.
2. Si l'autorité de certification est répertoriée, vérifiez qu'elle est correcte.

Problème 3: Expressway-E ne possède pas de domaine UC répertorié dans le SAN

Journaux des terminaux TC

```
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'
```

SAN Expressway-E

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

Correction

1. Régénérer Expressway-E CSR afin d'inclure les domaines UC.
2. Il est possible que sur le point de terminaison TC le paramètre **ExternalManager Domain** ne soit pas défini sur le domaine UC. Si c'est le cas, vous devez le faire correspondre.

Problème 4: Le nom d'utilisateur et/ou le mot de passe fournis dans le profil d'approvisionnement de TC est incorrect

Journaux des terminaux TC

```
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

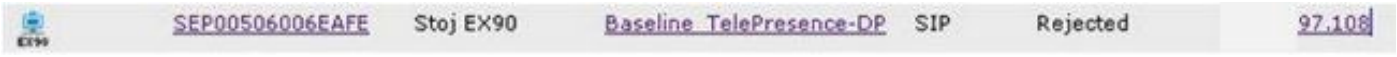
1. Vérifiez que le nom d'utilisateur/mot de passe saisi dans la page Provisioning du point de terminaison TC est valide.
2. Vérifiez les informations d'identification par rapport à la base de données CUCM.
3. Version 10 - Utiliser le portail Self Care
4. Version 9 - Utiliser les options utilisateur CM

L'URL des deux portails est la même : **https://%CUCM%/ucmuser/**

S'il y a une erreur de droits insuffisante, assurez-vous que ces rôles sont attribués à l'utilisateur :

- CTI standard activé
- Utilisateur final CCM standard

Problème 5: L'enregistrement des terminaux basé sur TC est rejeté



Traces 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 de terminaison TC

Expressway-C/VCS-C réel

```
X509v3 Subject Alternative Name:
DNS:RTP-TBTP-EXPRWY-C.tbtp.local, XMPP:conference-2-StandAloneCluster5ad9a.tbtp.local
```

Dans cet exemple de journal spécifique, il est clair que l'Expressway-C/VCS-C ne contient pas le nom de domaine complet du profil de sécurité du téléphone dans le SAN. (Secure-EX90.tbtp.local). Dans la prise de contact TLS (Transport Layer Security), le CUCM inspecte le certificat de serveur d'Expressway-C/VCS-C. Comme il ne le trouve pas dans le SAN, il affiche l'erreur en gras et signale qu'il attendait le profil de sécurité du téléphone au format FQDN.

Correction

1. Vérifiez que l'Expressway-C/VCS-C contient le profil de sécurité du téléphone au format FQDN dans le SAN de son certificat de serveur.
2. Vérifiez que le périphérique utilise le profil de sécurité correct dans CUCM si vous utilisez un profil sécurisé au format FQDN.
3. Cela peut également être dû au bogue Cisco ID CSCuq86376. Si tel est le cas, vérifiez la taille du SAN Expressway-C/VCS-C et la position du profil de sécurité du téléphone dans le SAN.

Problème 6: Échec du provisionnement des terminaux basé sur TC - Aucun serveur UDS

Cette erreur doit être présente sous **Diagnostics > Dépannage** :

```
Error: Provisioning Status
Provisioning failed: XML didnt contain UDS server addres
```

Journaux des terminaux TC

Faites défiler jusqu'à droite pour afficher les erreurs en gras

```
9685.56 PROV    REQUEST_EDGE_CONFIG:
9685.56 PROV    <?xml version='1.0' encoding='UTF-8'?>
9685.56 PROV    <getEdgeConfigResponse version="1.0"><serviceConfig><service><name>_cisco-phone-
tftp</name><error>NameError</error></service><service><name>_cuplogin</name><error>NameError</er
ror></service><service><name>_cisco-
uds</name><server><priority>1</priority><weight>1</weight><port>8443</port><address>cucm.domain.
int</address></server></service><service><name>tftpServer</name><address></address><address></ad
dress></service></serviceConfig><edgeConfig><sipEdgeServer><server><address>expe.domain.com</add
ress><tlsPort>5061</tlsPort></server></sipEdgeServer><sipRequest><route>&lt;sip:192.168.2.100:50
61;transport=tls;zone-
```

```
id=3;directed;lr&gt;</route></sipRequest><xmppEdgeServer><server><address>expe.domain.com</addre
ss><tlsPort>5222</tlsPort></server></xmppEdgeServer><httpEdgeServer><server><address>expe.domain
.com</address><tlsPort>8443</tlsPort></server></httpEdgeServer><turnEdgeServer/>



        </edgeConfig></getEdgeConfigResponse>
9685.57 PROV ERROR: Edge provisioning failed!
url='https://expe.domain.com:8443/ZXUuY2hlZ2cuY29t/get_edge_config/', message='XML didn't
contain UDS server address'
9685.57 PROV   EDGEProvisionUser: start retry timer for 15 seconds
9700.57 PROV I: [statusCheck] No active VcsE, reprovisioning!
```

Correction

1. Assurez-vous qu'un profil de service et un service CTI UC sont associés au compte d'utilisateur final utilisé pour demander le provisionnement des terminaux via les services MRA.

2. Accédez à **CUCM admin > User Management > User Settings > UC Service** et créez un service CTI UC qui pointe vers l'IP de CUCM (MRA_UC-Service).

3. Accédez à **CUCM admin > User Management > User Settings > Service Profile** et créez un nouveau profil (MRA_ServiceProfile).

4. Dans le nouveau profil de service, faites défiler jusqu'en bas et dans la section Profil CTI, sélectionnez le nouveau service CTI UC que vous venez de créer (c'est-à-dire MRA_UC-Service) , puis cliquez sur Enregistrer.

5. Accédez à **CUCM admin > User Management > End User** et recherchez le compte d'utilisateur utilisé pour demander le provisionnement des points de terminaison via les services MRA.

6. Sous **Paramètres** de **service** de cet utilisateur, assurez-vous que le cluster domestique est coché et que le profil de service UC reflète le nouveau profil de service que vous avez créé (c'est-à-dire MRA_ServiceProfile), puis cliquez sur Enregistrer.

7. La réplication peut prendre quelques minutes. Essayez de désactiver le mode de provisionnement sur le point de terminaison et de le réactiver quelques minutes plus tard pour voir si le point de terminaison s'enregistre maintenant.

Informations connexes

- Guide d'accès mobile et à distance
- Guide de création de certificat VCS
- Guide de démarrage EX90/EX60
- Guide de l'administrateur CUCM 9.1
- Support et documentation techniques - Cisco Systems