Résoudre les problèmes courants liés au renouvellement des certificats dans CUCM

Introduction

Ce document décrit les problèmes courants après la régénération des certificats dans Cisco Unified Communications Manager (CUCM) et comment les résoudre.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Processus de renouvellement des certificats CUCM
- Interface GUI de CUCM
- Serveurs Expressway
- Enregistrement des périphériques avec le processus CUCM
- Fonction Proxy De L'Autorité De Certification
- Guide de sécurité pour Cisco Unified Communications Manager

Composants utilisés

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

- CUCM version 15

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.

Impact commercial

Ce tableau affiche l'impact commercial de chaque renouvellement de certificat dans votre opération. Examinez attentivement les informations. Renouveler les certificats requis après les heures de bureau ou par périodes creuses, en fonction du niveau de risque de chaque certificat.

Low Impact Medium Impact. High Impact.

Type	Risk	Trust List	Impact	Phone Restart	Service Restart
Tomcat		-	Web services, SSO, EM/EMCC Login	None	Tomcat
IPSec		-	DRS, Ipsec Tunnels	None	DRF Master/Local
CAPF		CTL + ITL	LSC must be updated, secure features	All	CAPF
Callmanager		CTL + ITL	Registration, TL issues, Trunks, CTI	All	CM,CTI,TFTP
TVS		ITL	Verification of TLs, CFG files, https connection	Some	TVS
ITLRecovery		CTL + ITL	Signer or SAST backup for ITL/CTL	All	

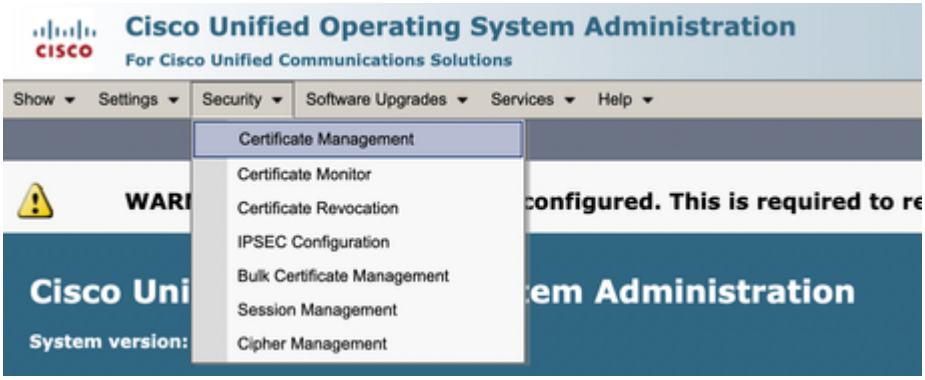
Scénario 1 : Les téléphones ne sont pas enregistrés après le renouvellement des certificats Call Manager, TVS et ITL

Remarque : Ce scénario s'applique aux déploiements sous des clusters CUCM en mode mixte et non sécurisé, en outre, s'applique aux certificats auto-signés et aux certificats CA.

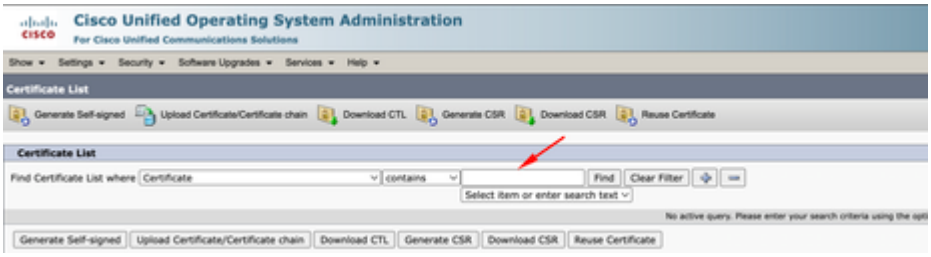
Lorsque les certificats Call Manager , TVS et ITL ont expiré et ont été renouvelés en même temps, il se produit que tous nos téléphones dans un état non enregistré qui entraîne un impact majeur sur le système, ce sont des comportements attendus que nous déclenchons les téléphones à ne pas faire confiance dans le CUCM.

Vérification

1. Assurez-vous que les certificats ont déjà expiré sous Cisco Unified OS Administration > Security > Certificate Management

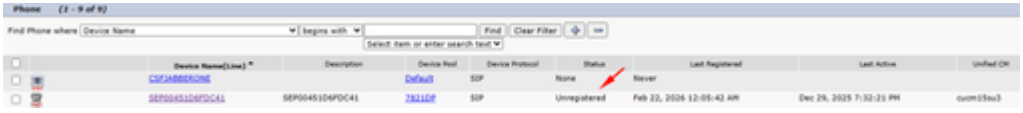


2. Effectuez une recherche par Callmanager, TVS ou ITL sous le filtre en haut de la page et utilisez les options Contient ou Commence par :



3. Les certificats doivent être mis à jour et vérifiés sous la colonne Expiration (identique pour les certificats TVS et ITL)

4. Une fois que vous avez vérifié que tout fonctionne correctement après le renouvellement du certificat, les téléphones sont affichés en tant qu'état Non enregistré.

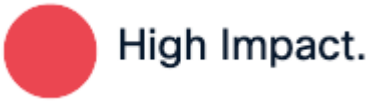


Solution

Il existe 2 options pour résoudre le problème :

1. Effectuez une réinitialisation d'usine du téléphone qui permet au téléphone d'effacer les paramètres de sécurité actuels et d'autoriser le téléphone à récupérer les nouveaux certificats
2. Mettez à jour les certificats ITL et CTL à partir de l'interface de ligne de commande sur le

noeud éditeur et utilisez la commande utils itl reset localkey.
Cette étape concerne tous les téléphones, y compris les téléphones enregistrés. Veillez à effectuer cette opération en dehors des heures de bureau.



Scénario 2 : l'authentification unique ne fonctionne pas après le renouvellement du certificat Tomcat

---

Remarque : Ce scénario peut s'appliquer aux déploiements qui utilisent un accord par noeud ou à l'échelle du cluster pour la configuration de l'authentification unique

---

Connexion dans CUCM avec authentification unique (SSO) : affiche un message d'erreur ¨Erreur lors du traitement de la réponse saml¨ ou ¨Erreur lors du traitement de la réponse saml Echec du déchiffrement de la clé secrète¨

Vérification

1. Assurez-vous que tous les noeuds contiennent un certificat tomcat valide s'ils sont auto-signés ou s'ils contiennent le nouveau certificat tomcat multi-san associé.
2. Utilisez set samltrace level debug dans tous les noeuds CUCM via CLI afin d'activer les journaux SSO sur le niveau de débogage
3. Recréez le problème en vous connectant à nouveau à CUCM et en utilisant la méthode SSO.
4. Collectez les journaux d'authentification unique de Tomcat après l'incident et vérifiez que vous obtenez ce message :
   -

```
2026-01-10 06:06:31,274 ERROR [http-nio-81-exec-157]  cpi.sso.saml.sp.security.authenticatio
com.sun.identity.saml2.common.SAML2Exception: Failed to decrypt the secret key.
              at com.sun.identity.saml2.xmlenc.FMEncProvider.getEncryptionKey(FMEncProvider.
              at com.sun.identity.saml2.xmlenc.FMEncProvider.decrypt(FMEncProvider.java:607)
              at com.sun.identity.saml2.assertion.impl.EncryptedAssertionImpl.decrypt(Encryp
...
```

Solution

Exportation des métadonnées CUCM après le renouvellement du certificat Tomcat et importation vers le serveur du fournisseur d'identité pour s'assurer qu'il dispose du nouveau certificat Tomcat pour cette communication.

Procédure de renouvellement de tomcat avec le déploiement SSO activé :

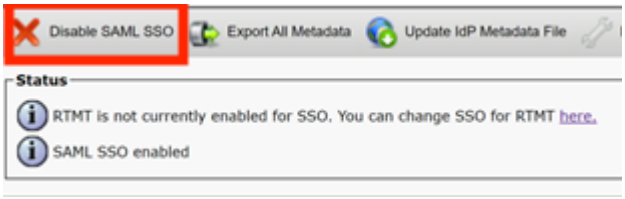
⚠ Mise en garde : Le Centre d'assistance technique (TAC) recommande les étapes suivantes afin d'éviter tout problème après le renouvellement du certificat Tomcat, recommande d'effectuer cette procédure après les heures de bureau.

Low Impact

1. Désactivez SSO dans tous les noeuds CUCM

- Accès à l'administration de CM > Système > Authentification unique SAML

- Sélectionnez Désactiver SAML SSO

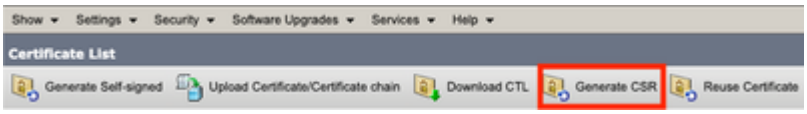


- Ce processus doit être effectué dans tous les autres noeuds via l'interface utilisateur graphique si un accord par noeud est utilisé.

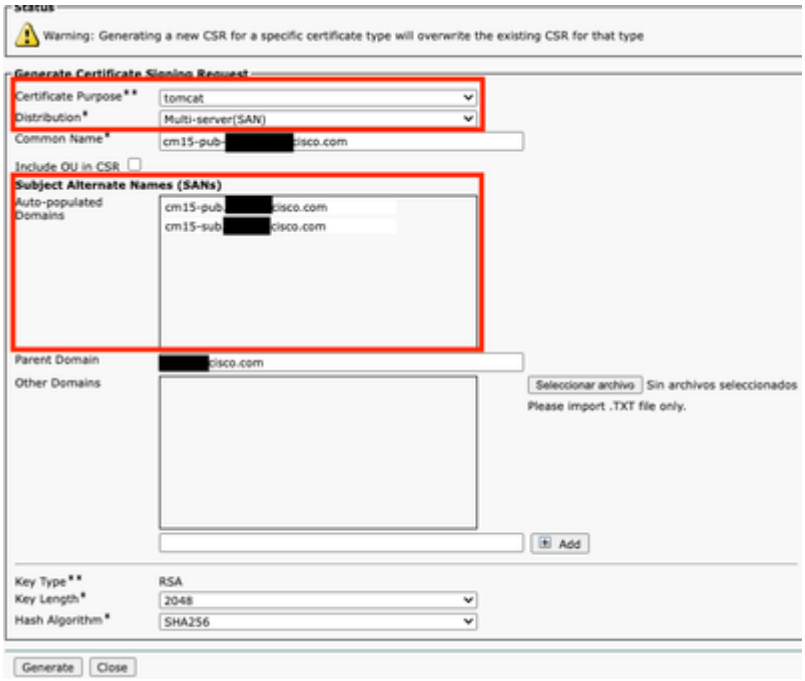
2. Renouveler le certificat Tomcat dans le cluster CUCM

Procédure globale de renouvellement du certificat multi-san Tomcat dans le cluster CUCM :

- Accédez à OS administration > Security > Certificate management.
- Sélectionnez Generate CSR (produire CSR).



- Sélectionnez Tomcat dans Certificate Propulse.
- Sélectionnez Multi-SAN dans Distribution.
- Assurez-vous que tous les noeuds du cluster sont répertoriés sous Domaines remplis automatiquement.



- Sélectionnez Générer. Assurez-vous que CSR est créé dans tous les noeuds du cluster.
- Téléchargez le CSR généré à partir de l'éditeur CUCM et signez-le avec un serveur d'autorité de certification (CA).
- Accédez à Administration du système d'exploitation > Sécurité > Gestion des certificats. Sélectionnez Télécharger le certificat/la chaîne de certificats.
- Téléchargez les certificats CA en tant que Tomcat-trust.
- Répétez l'étape 6 et téléchargez le certificat signé Tomcat en tant que Tomcat.
- Une fois terminé et vérifié que le nouveau certificat tomcat est appliqué à tous les noeuds, redémarrez le service Tomcat via l'interface de ligne de commande dans tous les noeuds du cluster à l'aide de cette commande jusqu'à ce que le service redémarre Cisco Tomcat.

Pour plus d'informations, reportez-vous à la documentation suivante :

- Régénérer le certificat auto-signé Tomcat
- Régénérez le certificat signé par l'autorité de certification Tomcat.

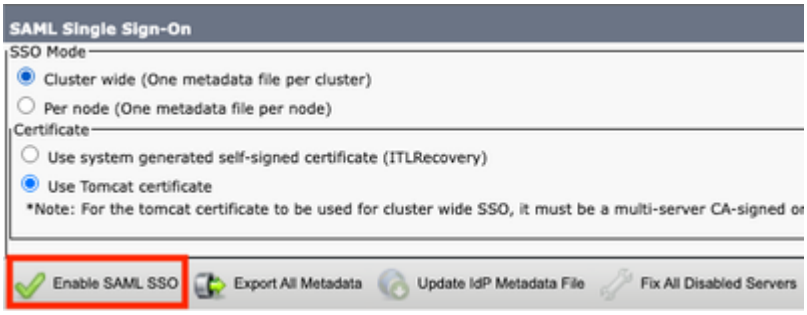
3. Exporter les métadonnées du fournisseur de services (SP)

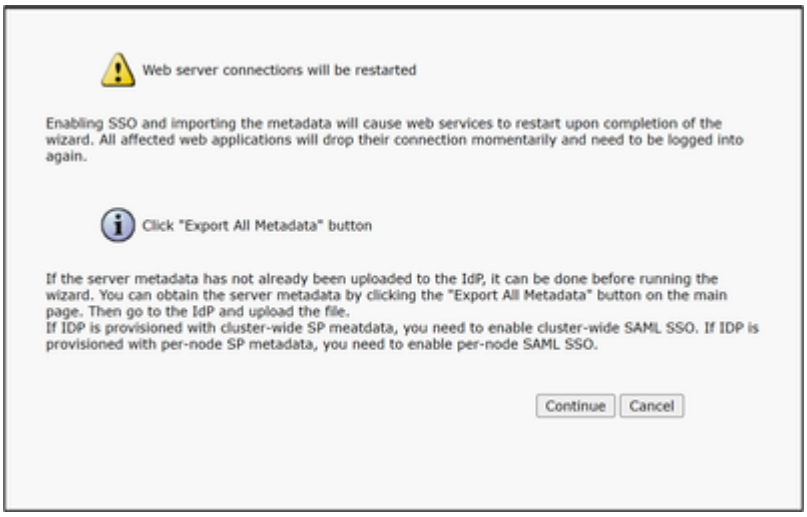
- Accédez à Administration CM > Système > Connexion unique
- Configurez les options SSO (dans ce cas, cluster wide en mode SSO et Use tomcat certificate on certificate is configured as a example), puis sélectionnez export all metadata

- Importez les métadonnées SP sur le serveur du fournisseur d'identités (IdP). Pour plus d'informations, référez-vous à Configurer SAML SSO sur Identity Provider

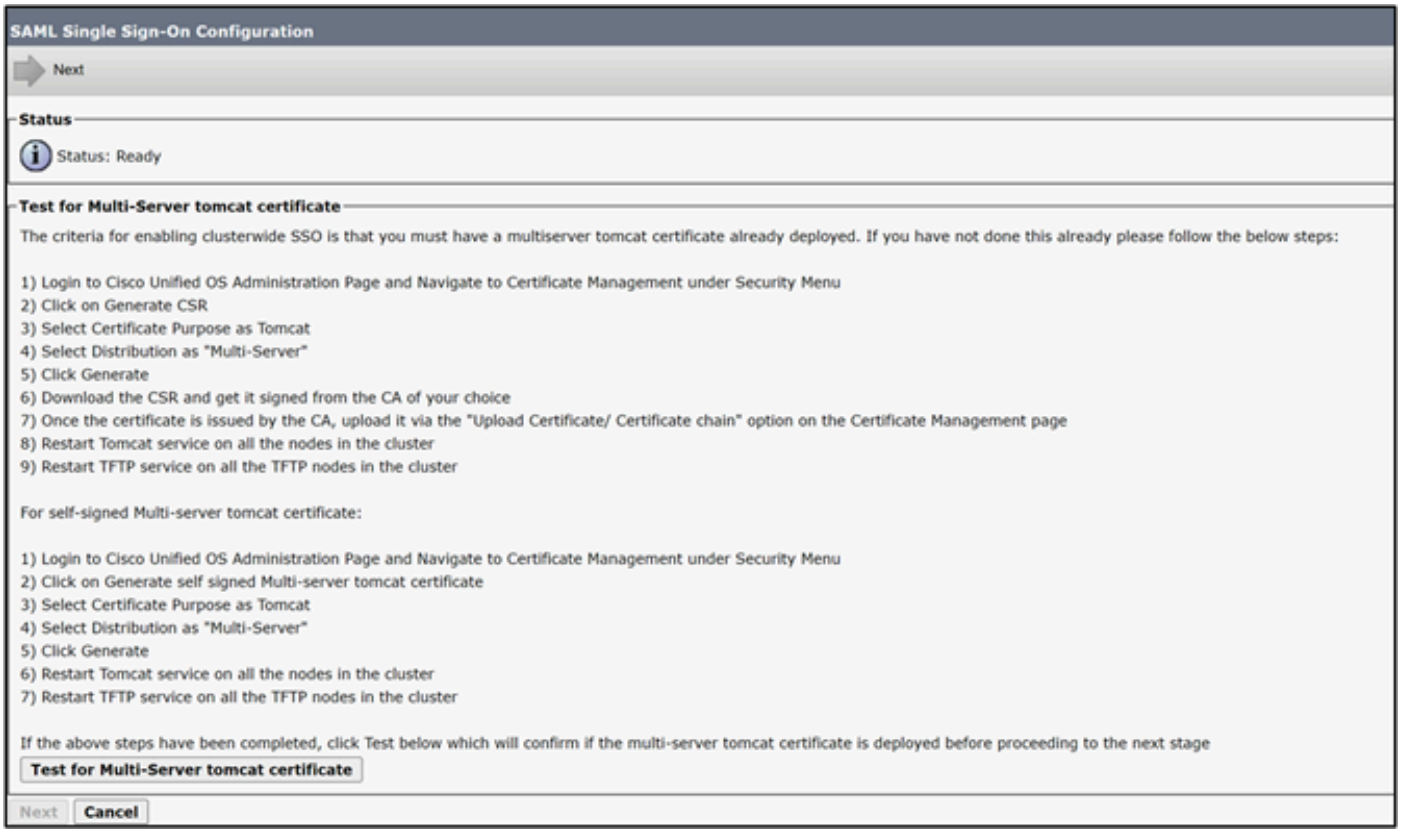
4. Activer SSO dans le cluster CUCM

- Accédez à Administration CM > Système > Connexion unique
- Avec les mêmes options SSO sélectionnées lors de l'exportation des métadonnées CUCM, sélectionnez Enable SAML SSO et sélectionnez continue.

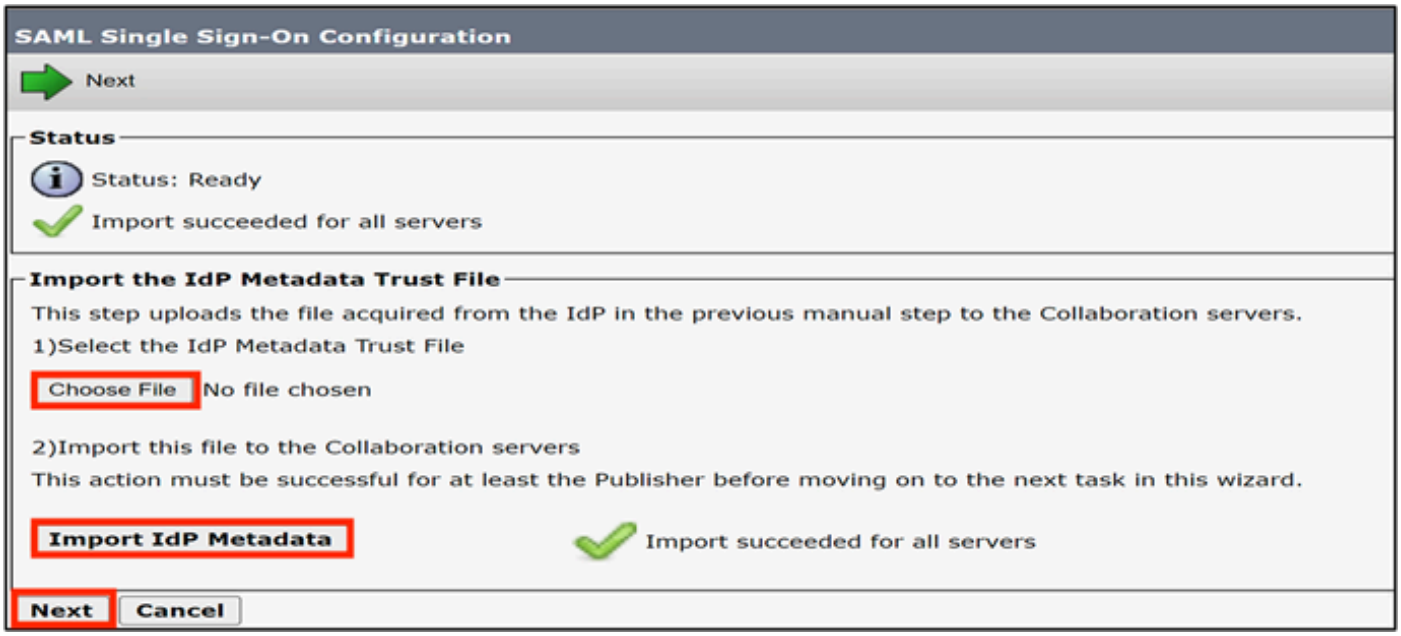




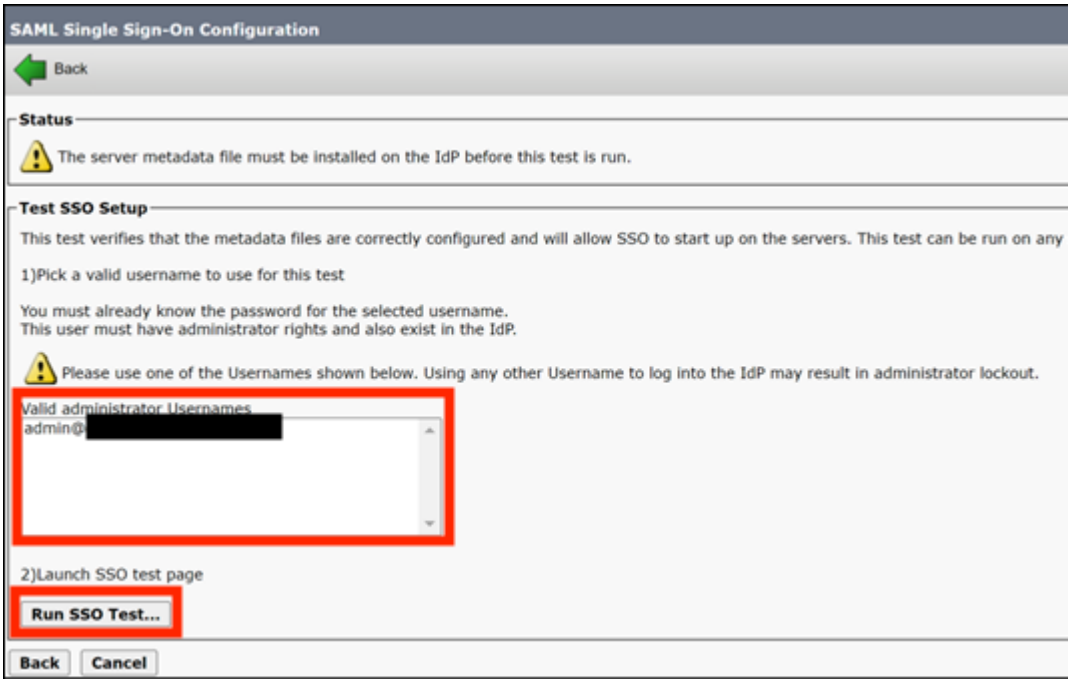
- Si cette étape est disponible à l'échelle du cluster pour vérifier le certificat multi-san dans tous les noeuds, sélectionnez Test for multi-server tomcat certificate. une fois terminé, sélectionnez Suivant.

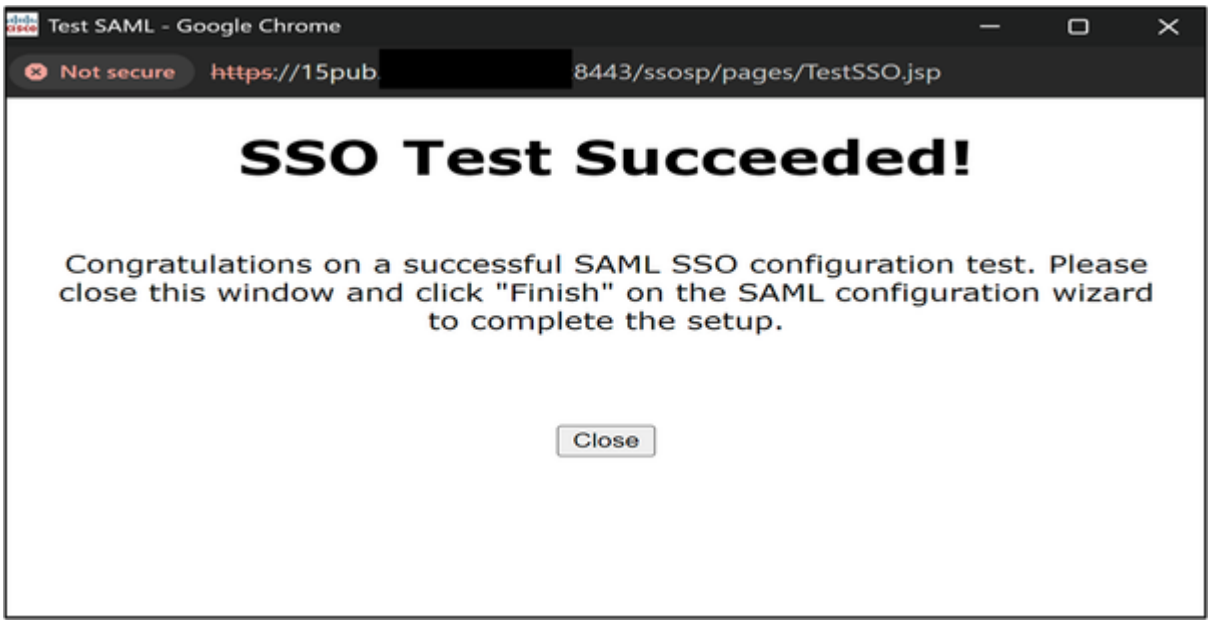


- Téléchargez les métadonnées IdP, sélectionnez Importer les métadonnées IdP et une fois terminé, sélectionnez Suivant



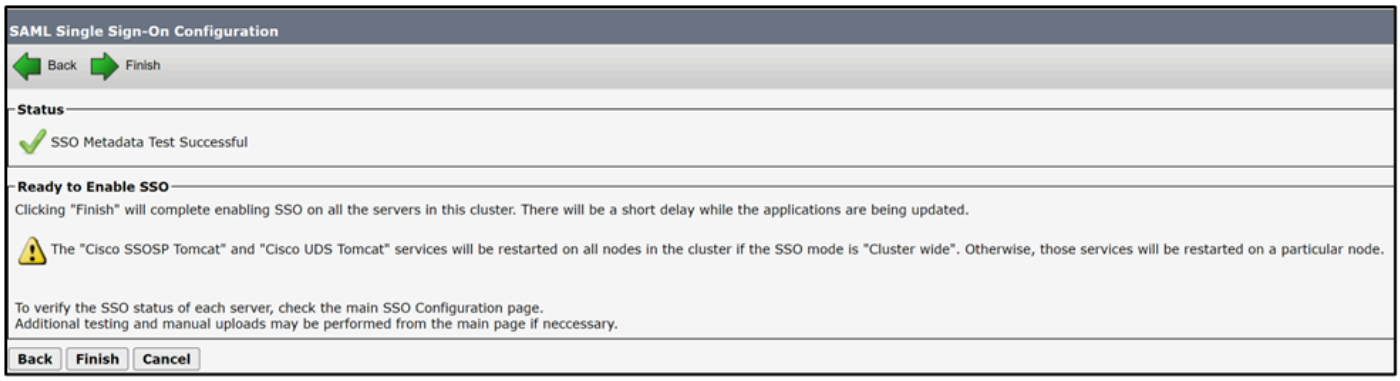
- Dans Test SSO Setup, sélectionnez un utilisateur auquel est affecté un groupe de super utilisateurs CCM standard, puis sélectionnez Run SSO Test jusqu'à ce que l'opération réussisse.





4. Redémarrez les services requis après l'activation de SSO.

- L'activation de SSO redémarre le service tomcat.



Cependant, le TAC recommande de redémarrer le service Tomcat (utils service restart Cisco Tomcat) et UDS Tomcat (utils service restart CiscoUDSTomcat) manuellement dans tous les noeuds après le processus d'activation SSO.

Scénario 3 : Problèmes d'enregistrement de mobilité et d'accès distant après le renouvellement du certificat

L'application Webex ne peut pas s'enregistrer auprès de CUCM via Mobility and Remote Access (MRA) après le renouvellement des certificats Call Manager, Tomcat et Expressway C sur les déploiements en mode mixte.

Vérification

1. Le gestionnaire d'appels CUCM et le certificat Tomcat sont des certificats signés CA.
2. Le déploiement de CUCM et d'Expressway s'exécute en mode mixte (TLS).
3. inspecter les journaux d'Expressway-C affiche « Routes SSL : ssl3_read_bytes : tlsv1 alert unknown ca ».
   <#root>

```
2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]: UTCTime="2026-01-29 19:01:16,974" Module
HTTPMSG:
|GET /CSFmarcoalh.cnf.xml HTTP/1.1
 Host: expc.cisco.com:6972
 Accept: */*
 Cookie:<CONCEALED>
 User-Agent: WebEx/0.0.0.0
 TrackingID: fxxxxxxx-86f6-4030-8259-0b768c07723e
 Client-ip: xxx.xxx.xxx.xxx
 X-Forwarded-For: xxx.xxx.xxx.xxx, 127.0.0.1
 Via: https/1.1 vcs[0fxxxxxx-c853-xxxx-aa16-0a290bf56fc8] (ATS), http/1.1 vcs[5xxxxxxx-7feb-4xxx-9

 |

2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]:[ET_NET 1]ERROR:SSL connection failed for

SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca
```

Solution

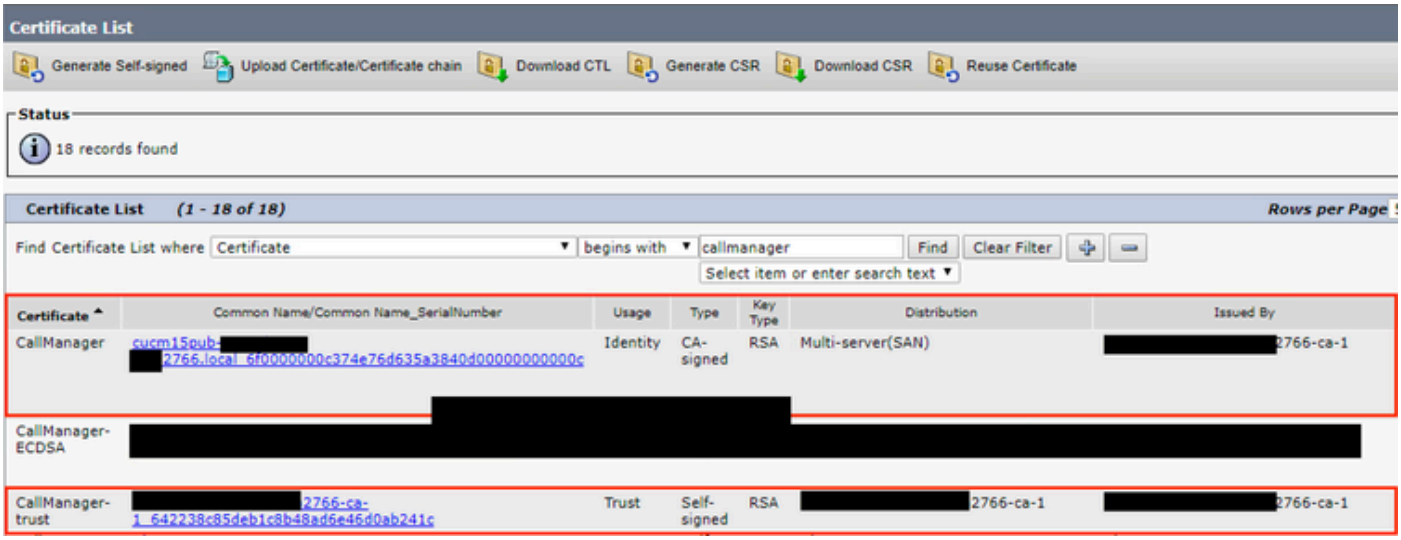
Exporter et importer des certificats entre CUCM et Expressway-C pour assurer une relation de confiance.

⚠ Mise en garde : Le TAC recommande d'effectuer cette opération en dehors des heures de bureau, car cette procédure nécessite le redémarrage des services. Impact commercial :

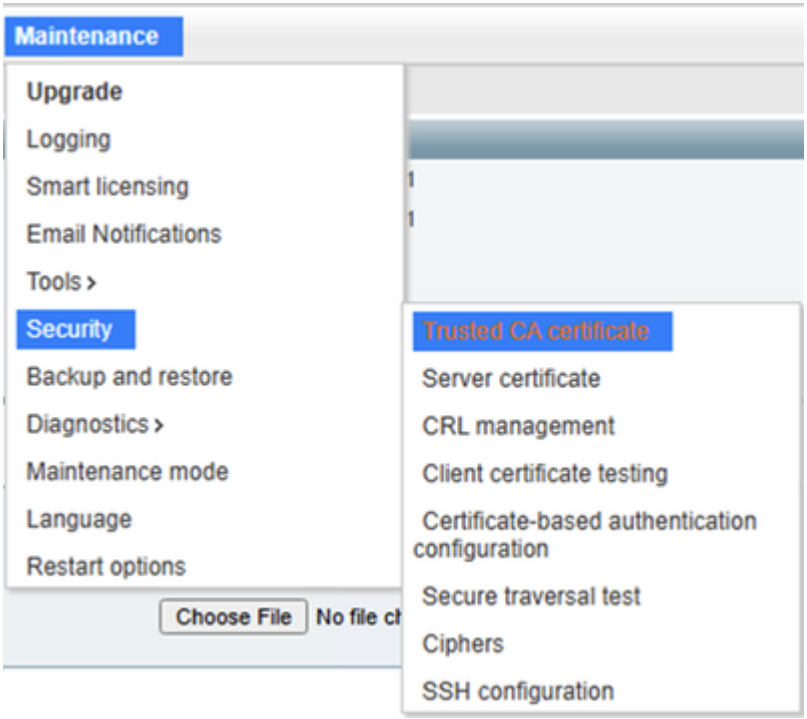
Medium Impact.

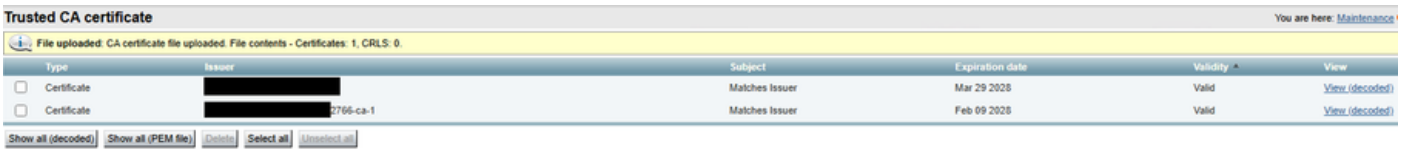
1. Procédure pour compléter la relation de confiance entre CUCM et Expressway avec les certificats signés CA

Accédez à OS administration > Security > Certificate management et téléchargez le certificat CA racine et le certificat intermédiaire (le cas échéant) qui signe Call Manager et le certificat Tomcat.



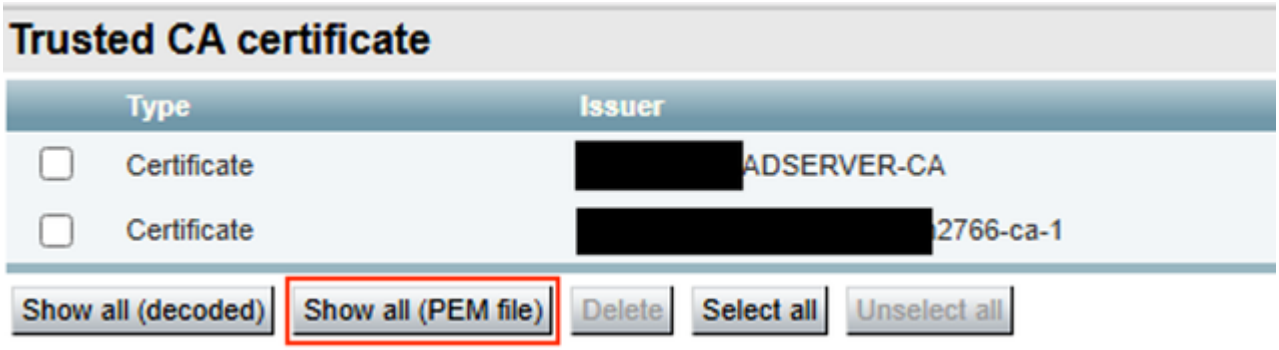
Accédez ensuite à Expressway-C > Maintenance > Security > Trusted CA certificate et téléchargez le certificat CA de Call Manager et le certificat Tomcat.



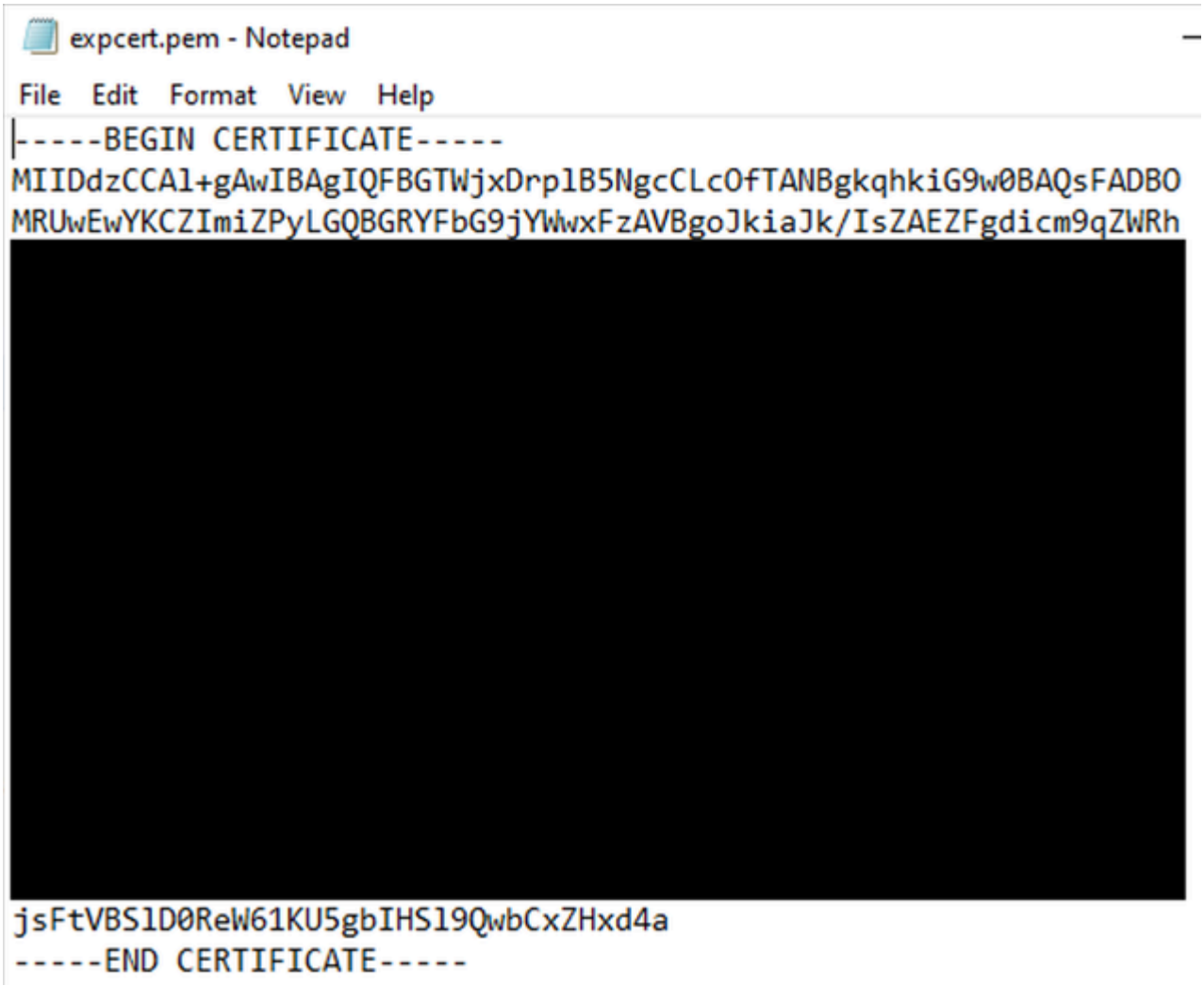


Remarque : Dans les scénarios où Call Manager et le certificat Tomcat sont auto-signés, téléchargez le vrai certificat Call Manager et Tomcat et téléchargez-le sur Expressway.

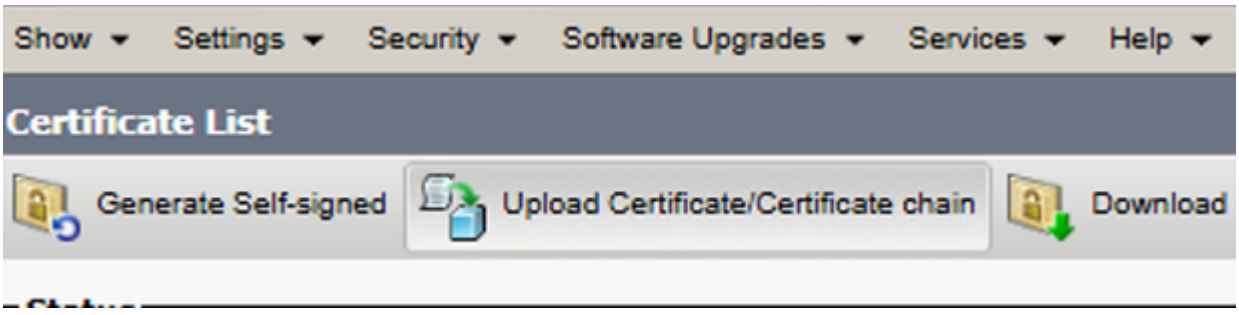
Accédez à Expressway-C > Maintenance > Security > Trusted CA certificate > Show all (PEM file)

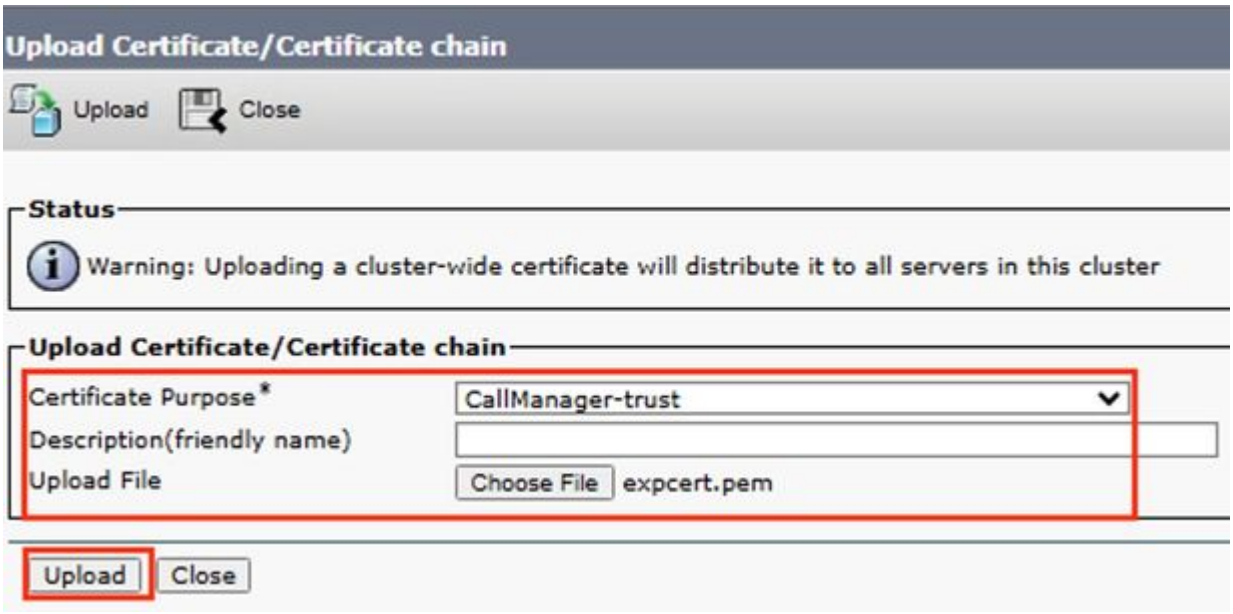


Copiez la valeur PEM du certificat CA qui signe Expressway-C et enregistrez-la dans un fichier texte.



Accédez à OS administration > Security > Certificate management et sélectionnez Upload Certificate/Certificate Chain et téléchargez le certificat AC expressway-C comme Tomcat-trust et Call Manager-trust





Redémarrer les services requis dans le cluster CUCM :

- Accédez à Cisco Unified Serviceability > Tools > Control Center - Feature Services et redémarrez le service Cisco CallManager dans tous les noeuds qui l'exécutent.
- Accédez à Cisco Unified Serviceability > Tools > Control Center - Feature Services et redémarrez le service Cisco TFTP dans tous les noeuds qui l'exécutent.
- Redémarrez le service Tomcat dans tous les noeuds du cluster via l'interface de ligne de commande avec la commande utils service restart Cisco Tomcat.
- Redémarrez le service Cisco HAproxy dans tous les noeuds du cluster via l'interface de ligne de commande avec la commande utils service restart Cisco HAProxy.

Scénario 4 : Renouvellement de la cause de certificat de fonction proxy d'autorité de certification

Scénario 4.1 : Échec de l'authentification 802.1x

Le téléphone ne s'authentifie pas avec ASA après la régénération du certificat CAPF (Certificate Authority Proxy Function) sur l'éditeur CUCM.

Vérification

1. Les messages d'état du téléphone indiquent « Authentification 802.1x : Échec"

2. Inspectez les journaux téléphoniques du serveur affecté et recherchez « SSL_ERROR_WANT_READ »

```
4592 NOT Feb 17 11:01:25.041733 (349-349) PAE: -Secure Connection Handshake in progress - status SSL_ERR
4593 NOT Feb 17 11:01:25.041826 (349-349) PAE: -EV_REQUEST_REC, ST_AUTHENTICATING->ST_AUTHENTICATING
++ EAP-Failure
4594 NOT Feb 17 11:01:25.041898 (349-349) PAE: -send EAP-Resp/TLS - id 9
4595 NOT Feb 17 11:01:25.042032 (349-349) PAE: -authWhile timer set: 30 sec
4596 NOT Feb 17 11:01:27.061822 (349-349) PAE: -[0001-0] 08-cc-a7-1c-bb-ae vid=0xfff=4095 static=0 pri=0
4597 NOT Feb 17 11:01:27.061950 (349-349) PAE: -port=0
4598 NOT Feb 17 11:01:27.062009 (349-349) PAE: -cprCdpGetPort address:  8:CC:A7:1C:BB:AE  Phyport=0 appP
4599 NOT Feb 17 11:01:27.062068 (349-349) PAE: - >>>>>>>>>>>>>> port obtained = 0 for mac macAddress 08:c
4600 NOT Feb 17 11:01:27.062134 (349-349) PAE: -rcvd EAP-Failure
4601 NOT Feb 17 11:01:27.062189 (349-349) PAE: -EV_FAILURE, ST_AUTHENTICATING->ST_HELD
4602 WRN Feb 17 11:01:27.062462 (349-349) PAE: -802.1X auth FAILED
4603 NOT Feb 17 11:01:27.062550 (349-349) PAE: -paeInfoToInetd: PAE info sent to NETSD
4604 NOT Feb 17 11:01:27.062717 (1786-1880) JAVA-Calling handleNetSDEvent
4605 WRN Feb 17 11:01:27.062953 (1786-1880) JAVA-Thread-11|cip.sec.Security:? - Security: Received a pro
4606 DEB Feb 17 11:01:27.063039 (1786-1880) JAVA-openQue(): que->/tmp/pae_msg_que, key->0x101019ab
4607 DEB Feb 17 11:01:27.063069 (1786-1880) JAVA-openQue(): que->/tmp/pae_rsp_que, key->0x10101c4c
4608 DEB Feb 17 11:01:27.063091 (1786-1880) JAVA-getpaeinfo: send pae info message paeCmd.mtype=1880, pa
4609 DEB Feb 17 11:01:27.063121 (1786-1880) JAVA-getpaeinfo: recv pae info resp ret=-1, errno=No message
4610 NOT Feb 17 11:01:27.063306 (349-349) PAE: -paeInfoToInetd: Netsd event NETSD_EV_PAE sent to NETSD
4611 NOT Feb 17 11:01:27.063370 (349-349) PAE: - PAE RE-AUTH, not sending SEC_DOWN Netsd event for CDP
4612 NOT Feb 17 11:01:27.063423 (349-349) PAE: -paeSetLastSupStatus: LastSupStatus 0
4613 NOT Feb 17 11:01:27.063475 (349-349) PAE: -heldWhile timer set: 60 sec
4614 NOT Feb 17 11:01:27.064074 (349-349) PAE: -paeNetsdRcvMsg(349): PAE event: status: FAIL : Resource
```

Solution

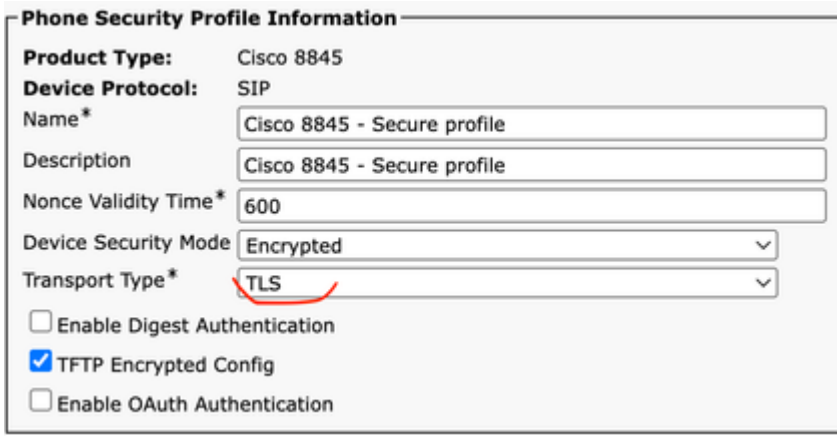
Téléchargez le certificat CAPF à partir de l'éditeur CUCM et téléchargez-le sur le serveur d'authentification, contournez la norme 802.1x pour permettre l'enregistrement et installer le certificat LSC sur les téléphones concernés.

Scénario 4.2 : Les téléphones ne sont pas enregistrés auprès de CUCM qui utilise un profil de sécurité en mode TLS.

Les téléphones affichent « Le téléphone est en cours d'enregistrement » après la régénération du certificat CAPF sur l'éditeur CUCM.

Vérification

1. Les téléphones affectés contiennent un profil de sécurité avec le mode TLS activé.



2. Les téléphones affectés ont un certificat LSC installé.
3. Assurez-vous que le certificat CAPF est à jour.

4. Connectez-vous à CUCM publisher et utilisez la commande show ctl qui affiche l'ancien numéro de série du certificat CAPF.
5. Modifiez ensuite le profil de sécurité du téléphone sur non sécurisé.

Solution

Régénérez le fichier CTL sur CUCM et redémarrez les services requis pour que les téléphones reçoivent le nouveau fichier CTL avec le fichier CAPF.

⚠ Mise en garde : Le TAC recommande d'effectuer cette opération en dehors des heures de bureau, car cette procédure nécessite le redémarrage des services. Impact commercial :

Medium Impact.

Une marche à suivre pour assurer le renouvellement du FPCA.


```
admin:utils ctl update CTLFile
This operation will update the CTLFile. Do you want to continue? (y/n): y

Updating CTL file
CTL file Updated
Please reset all Encrypted and Authenticated phones for the CTL file updates to take effect.
```

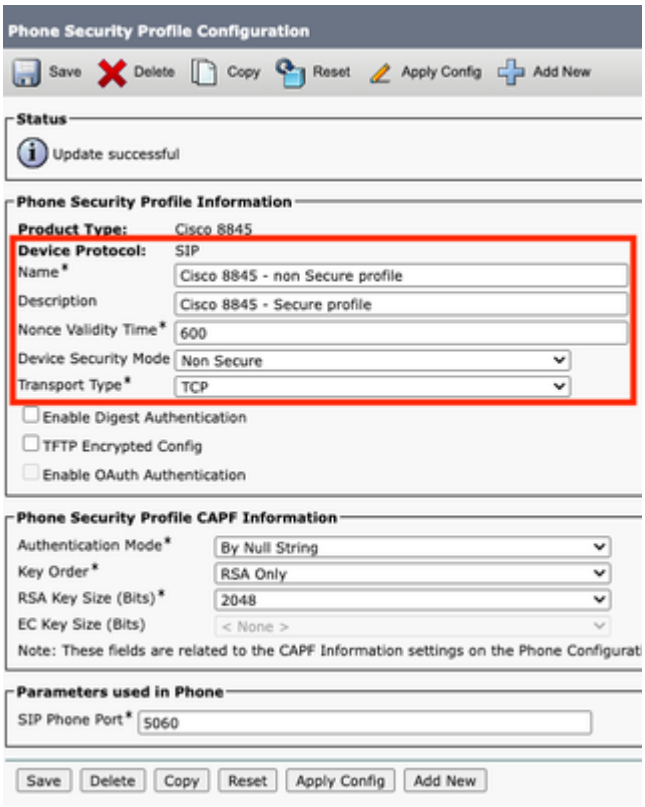
Mettez à jour le fichier CTL après la régénération CAPF. Connectez-vous à l'interface de ligne de commande du serveur de publication et entrez la commande utils ctl update CTLFile.

1. Accédez à Cisco Unified Serviceability > Tools > Control Center - Feature Services dans CUCM publisher et redémarrez le service CAPF.
2. Accédez à Cisco Unified Serviceability > Tools > Control Center - Network Services et redémarrez Cisco Trust Verification Service dans tous les noeuds qui l'exécutent.
3. Accédez à Cisco Unified Serviceability > Tools > Control Center - Feature Services et redémarrez Cisco TFTP Service dans tous les noeuds qui l'exécutent

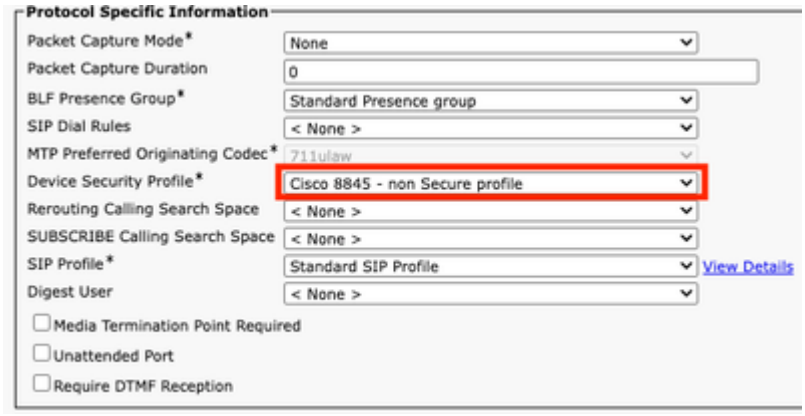
- Accédez à CM administration > System > Security > Phone Security Profile.

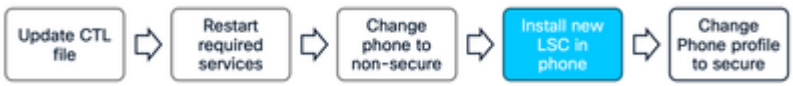
- Copiez le profil de sécurité téléphonique actuel affecté aux téléphones requis.

- Changez Name and Device Security Mode en Non Secure et sélectionnez Save and Apply Config pour appliquer cette modification à tous les téléphones requis.



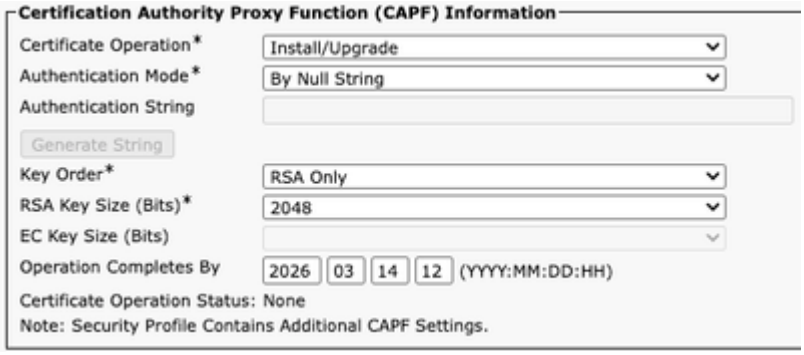
- Appliquez le profil de sécurité de périphérique créé à la configuration de téléphones requise, sélectionnez Save and Apply Config.





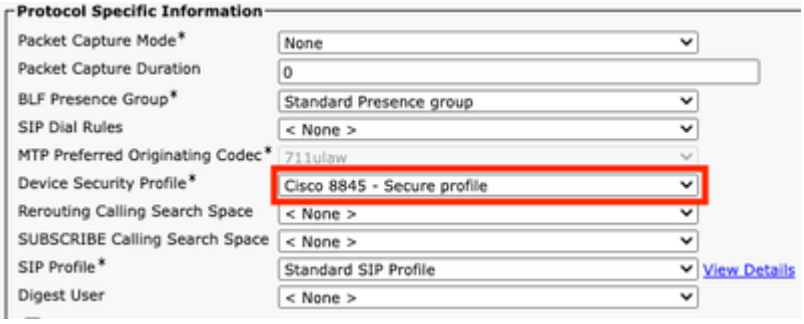
Utilisez la section des informations CAPF dans la configuration des périphériques des téléphones concernés pour installer le certificat LSC dans les téléphones requis.

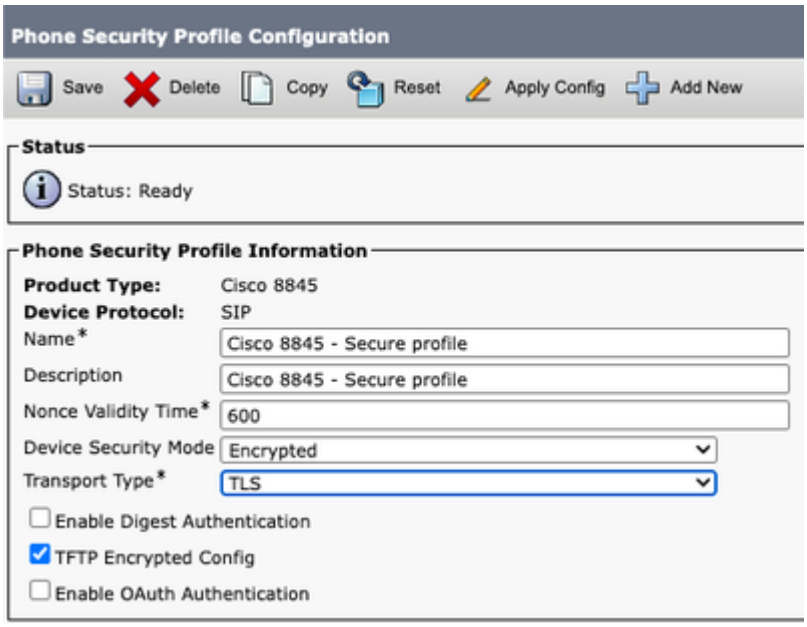
- Dans les informations CAPF, sélectionnez Install/Upgrade in Certificate Operation.



- Sélectionnez Save and Apply Config.
- Patientez jusqu'à ce que Certificate Operation Status affiche Operation completed.

Dans la section Informations spécifiques au protocole sur Configuration du téléphone, sélectionnez le profil de sécurité avec TLS activé qui a été créé.





Informations connexes

- https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/214231-certificate-regeneration-process-for-cis.html
- https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/217138-regeneration-of-cucm-ca-signed-certifica.html
- https://www.cisco.com/c/en/us/support/docs/content-networking/certificates/213295-how-to-install-an-lsc-on-a-cisco-ip-phon.html
- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X15-2/mra/exwy_b_mra-deployment-guide-x152.html

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.