Configuration de LSC sur un téléphone IP avec CUCM

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

- Comparaison des MIC et des LSC

Configurer

- Topologie du réseau

Vérifier

Installation LSC en bloc

Dépannage

- Aucun serveur CAPF valide
- LSC : Échec de connexion
- LSC : Échec
- LSC : Opération en attente

Informations connexes

Introduction

Ce document décrit comment installer un certificat important localement (LSC) sur un téléphone IP Cisco (téléphone IP Cisco).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Options du mode de sécurité du cluster Cisco Unified Communications Manager (CUCM)
- Certificats X.509
- Certificats de fabrication installés (MIC)

- LSC
- Opérations de certificat CAPF (Certificate Authority Proxy Function)
- Sécurité par défaut (SBD)
- Fichiers de la liste de confiance initiale (ITL)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de CUCM qui prennent en charge SBD, à savoir CUCM 8.0(1) et versions ultérieures.

Remarque : Elle concerne uniquement les téléphones qui prennent en charge la sécurité par défaut (SBD). Par exemple, les téléphones 7940 et 7960 ne prennent pas en charge SBD, pas plus que les téléphones de conférence 7935, 7936 et 7937. Pour obtenir la liste des périphériques qui prennent en charge SBD dans votre version de CUCM, accédez à Cisco Unified Reporting > System Reports > Unified CM Phone Feature List et exécutez un rapport sur Feature : Sécurité Par Défaut.

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

Le service Cisco Authority Proxy Function (CAPF) s'exécute uniquement sur le noeud éditeur. L'éditeur agit en tant qu'autorité de certification (CA) ou signataire du LSC.

Comparaison des MIC et des LSC

Si vous utilisez l'authentification basée sur certificat pour le VPN téléphonique 802.1X ou AnyConnect, il est important de comprendre la différence entre les MIC et les LSC.

Chaque téléphone Cisco est livré avec un MIC préinstallé en usine. Ce certificat est signé par l'un des certificats d'autorité de certification de fabrication Cisco, soit par le certificat d'autorité de certification de fabrication Cisco, soit par le certificat d'autorité de certification de fabrication Cisco SHA2, CAP-RTP-001 ou CAP-RTP-002. Lorsque le téléphone présente ce certificat, il prouve qu'il s'agit d'un téléphone Cisco valide, mais cela ne valide pas que le téléphone appartient à un utilisateur spécifique ou à un cluster CUCM. Il peut s'agir d'un téléphone non autorisé acheté sur le marché libre ou transféré d'un autre site.

Les LSC, quant à eux, sont volontairement installés sur les téléphones par un administrateur et sont signés par le certificat CAPF de l'éditeur CUCM. Vous configureriez un VPN 802.1X ou AnyConnect pour faire uniquement confiance aux LSC émis par les autorités de certification CAPF connues. Baser l'authentification de certificat sur des LSC plutôt que sur des MIC vous offre un contrôle beaucoup plus granulaire sur les périphériques téléphoniques approuvés.

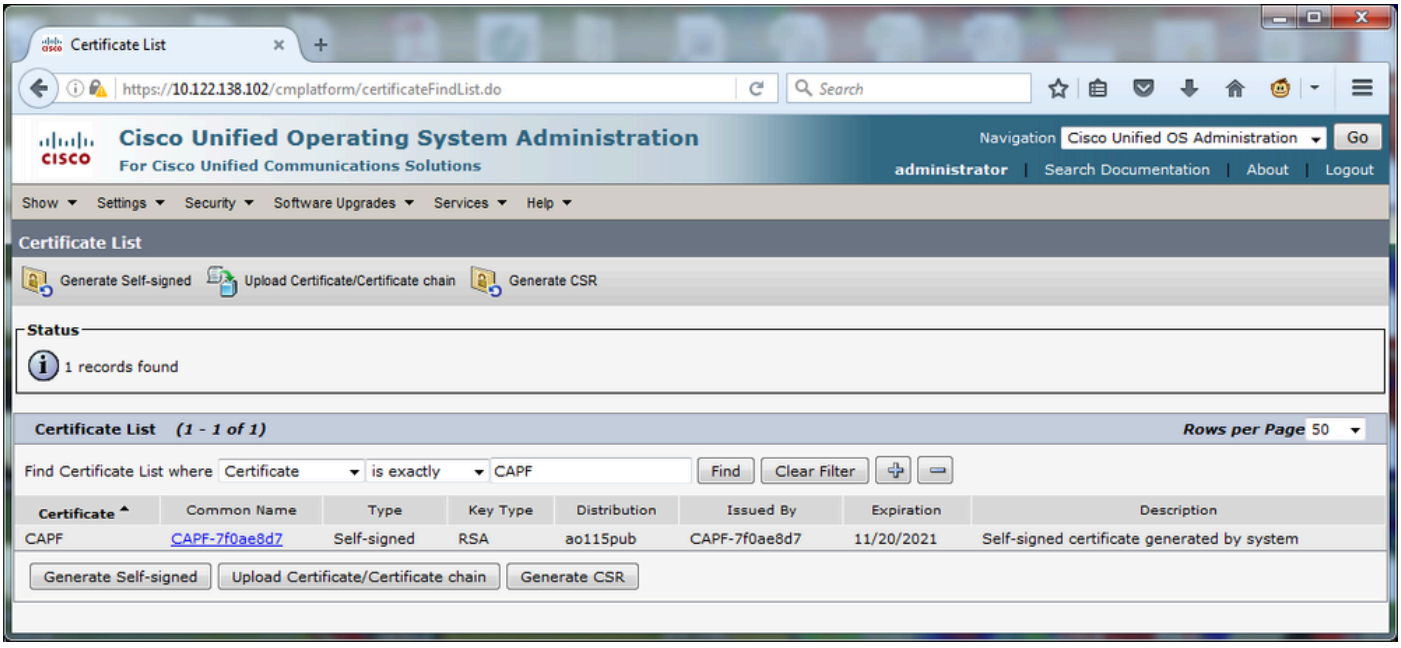
Configurer

Topologie du réseau

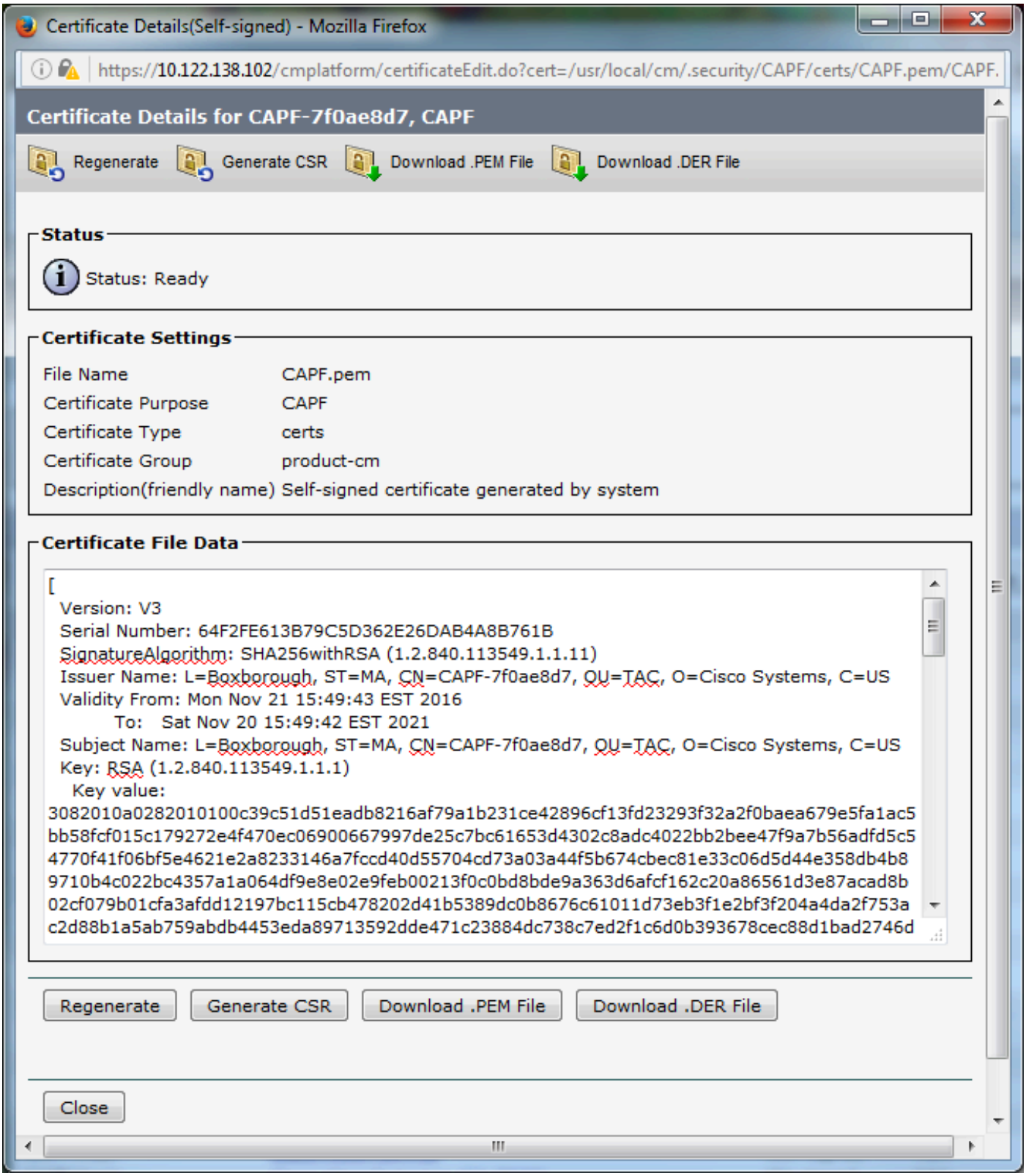
Les serveurs de travaux pratiques CUCM suivants ont été utilisés pour ce document :

- Serveur de publication CUCM et serveur TFTP
- Abonné CUCM et serveur TFTP

Vérifiez que le certificat CAPF n'a pas expiré et qu'il n'est pas sur le point d'expirer dans un avenir proche. Accédez à Cisco Unified OS Administration > Security > Certificate Management, puis Find Certificate List où Certificate est exactement CAPF comme indiqué dans l'image.



Cliquez sur Common Name afin d'ouvrir la page Certificate Details. Vérifiez la validité à partir de : et à : dans le volet Données du fichier de certificat afin de déterminer quand le certificat expire, comme illustré dans l'image.



Si le certificat CAPF a expiré ou arrive bientôt à expiration, régénérez ce certificat. Ne poursuivez pas le processus d'installation de LSC avec un certificat CAPF expiré ou sur le point d'expirer. Cela évite de devoir réémettre des LSC dans un avenir proche en raison de l'expiration du certificat CAPF. Pour plus d'informations sur la façon de régénérer le certificat CAPF, consultez l'article Processus de régénération/renouvellement de certificat CUCM.

De même, si vous devez faire signer votre certificat CAPF par une autorité de certification tierce,

vous avez un choix à faire à ce stade. Terminez maintenant la génération du fichier de demande de signature de certificat (CSR) et l'importation du certificat CAPF signé, ou continuez la configuration avec un LSC auto-signé pour un test préliminaire. Si vous avez besoin d'un certificat CAPF signé par un tiers, il est généralement judicieux de configurer d'abord cette fonctionnalité avec un certificat CAPF auto-signé, de tester et de vérifier, puis de redéployer les LSC qui sont signés par un certificat CAPF signé par un tiers. Cela simplifie le dépannage ultérieur, si les tests avec le certificat CAPF signé par un tiers échouent.

Avertissement : Si vous régénérez le certificat CAPF ou importez un certificat CAPF signé par un tiers alors que le service CAPF est activé et démarré, les téléphones sont automatiquement réinitialisés par CUCM. Effectuez ces procédures dans une fenêtre de maintenance lorsqu'il est acceptable de réinitialiser des téléphones. Pour référence, consultez l'ID de bogue Cisco CSCue55353 - Ajouter un avertissement lors de la régénération du certificat TVS/CCM/CAPF que les téléphones réinitialisent

---

Remarque : Si votre version de CUCM prend en charge SBD, cette procédure d'installation LSC s'applique, que votre cluster CUCM soit défini en mode mixte ou non. SBD fait partie de CUCM version 8.0(1) et ultérieure. Dans ces versions de CUCM, les fichiers ITL contiennent le certificat pour le service CAPF sur le serveur de publication CUCM. Cela permet aux téléphones de se connecter au service CAPF afin de prendre en charge les opérations de certificat telles que l'installation/mise à niveau et le dépannage.

Dans les versions précédentes de CUCM, il était nécessaire de configurer le cluster pour le mode mixte afin de prendre en charge les opérations de certificat. Comme cela n'est plus nécessaire, cela réduit les obstacles à l'utilisation des LSC comme certificats d'identité de téléphone pour l'authentification 802.1X ou pour l'authentification de client VPN AnyConnect.

Exécutez la commande show itl sur tous les serveurs TFTP dans le cluster CUCM. Notez que le fichier ITL contient un certificat CAPF.

Par exemple, voici un extrait de la sortie de show itl du TP Abonné CUCM ao115sub.

Remarque : Ce fichier contient une entrée d'enregistrement ITL avec une fonction CAPF.

Remarque : Si votre fichier ITL n'a pas d'entrée CAPF, connectez-vous à votre éditeur CUCM et confirmez que le service CAPF est activé. Afin de confirmer cela, naviguez vers Cisco Unified Serviceability > Tools > Service Activation > CUCM Publisher > Security, puis activez le Cisco Certificate Authority Proxy Function Service. Si le service a été désactivé et que vous venez de l'activer, accédez à Cisco Unified Serviceability > Tools > Control Center - Feature Services > Server > CM Services, puis redémarrez le service Cisco TFTP sur tous

---

les serveurs TFTP dans le cluster CUCM pour régénérer le fichier ITL. Assurez-vous également de ne pas taper l'ID de bogue Cisco CSCuj78330.

Remarque : une fois que vous avez terminé, exécutez la commande show itl sur tous les serveurs TFTP dans le cluster CUCM afin de vérifier que le certificat CAPF du serveur de publication CUCM actuel est maintenant inclus dans le fichier.

<#root>

```
 ITL Record #:1


 ----


BYTEPOS TAG LENGTH VALUE


------- --- ------ -----


1 RECORDLENGTH 2 727


2 DNSNAME 2


3 SUBJECTNAME 64 CN=CAPF-7f0ae8d7;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US


4 FUNCTION 2 CAPF


5 ISSUERNAME 64 CN=CAPF-7f0ae8d7;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US


6 SERIALNUMBER 16 64:F2:FE:61:3B:79:C5:D3:62:E2:6D:AB:4A:8B:76:1B
```

7 PUBLICKEY 270

8 SIGNATURE 256

11 CERTHASH 20 C3 E6 97 D0 8A E1 0B F2 31 EC ED 20 EC C5 BC 0F 83 BC BC 5E

12 HASH ALGORITHM 1 null

```
 ITL Record #:2
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 717
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 59 CN=ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 6B:99:31:15:D1:55:5E:75:9C:42:8A:CE:F2:7E:EA:E8
7 PUBLICKEY 270
8 SIGNATURE 256
11 CERTHASH 20 05 9A DE 20 14 55 23 2D 08 20 31 4E B5 9C E9 FE BD 2D 55 87
12 HASH ALGORITHM 1 null

 ITL Record #:3
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1680
2 DNSNAME 2
3 SUBJECTNAME 71 CN=ITLRECOVERY_ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 71 CN=ITLRECOVERY_ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 51:BB:2F:1C:EE:80:02:16:62:69:51:9A:14:F6:03:7E
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 963 DF 98 C1 DB E0 61 02 1C 10 18 D8 BA F7 1B 2C AB 4C F8 C9 D5 (SHA1 Hash HEX)
This etoken was not used to sign the ITL file.

 ITL Record #:4
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 717
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 65:E5:10:72:E7:F8:77:DA:F1:34:D5:E3:5A:E0:17:41
```

```
7 PUBLICKEY 270
8 SIGNATURE 256
11 CERTHASH 20 00 44 54 42 B4 8B 26 24 F3 64 3E 57 8D 0E 5F B0 8B 79 3B BF
12 HASH ALGORITHM 1 null

 ITL Record #:5
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1652
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 48:F7:D2:F3:A2:66:37:F2:DD:DF:C4:7C:E6:B9:CD:44
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 959 20 BD 40 75 51 C0 61 5C 14 0D 6C DB 79 E5 9E 5A DF DC 6D 8B (SHA1 Hash HEX)
This etoken was used to sign the ITL file.

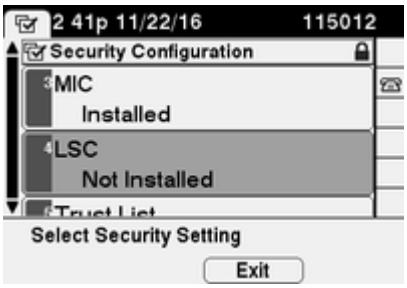
 ITL Record #:6
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1652
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TFTP
5 ISSUERNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 48:F7:D2:F3:A2:66:37:F2:DD:DF:C4:7C:E6:B9:CD:44
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 959 20 BD 40 75 51 C0 61 5C 14 0D 6C DB 79 E5 9E 5A DF DC 6D 8B (SHA1 Hash HEX)

 ITL Record #:7
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1031
2 DNSNAME 9 ao115sub
3 SUBJECTNAME 62 CN=ao115sub-EC;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TFTP
5 ISSUERNAME 62 CN=ao115sub-EC;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 53:CC:1D:87:BA:6A:28:BD:DA:22:B2:49:56:8B:51:6C
7 PUBLICKEY 97
8 SIGNATURE 103
9 CERTIFICATE 651 E0 CF 8A B3 4F 79 CE 93 03 72 C3 7A 3F CF AE C3 3E DE 64 C5 (SHA1 Hash HEX)

The ITL file was verified successfully.
```

Une fois l'entrée CAPF confirmée comme entrée dans l'ITL, vous pouvez effectuer une opération de certificat sur un téléphone. Dans cet exemple, un certificat RSA de 2048 bits est installé à l'aide de l'authentification Null String.

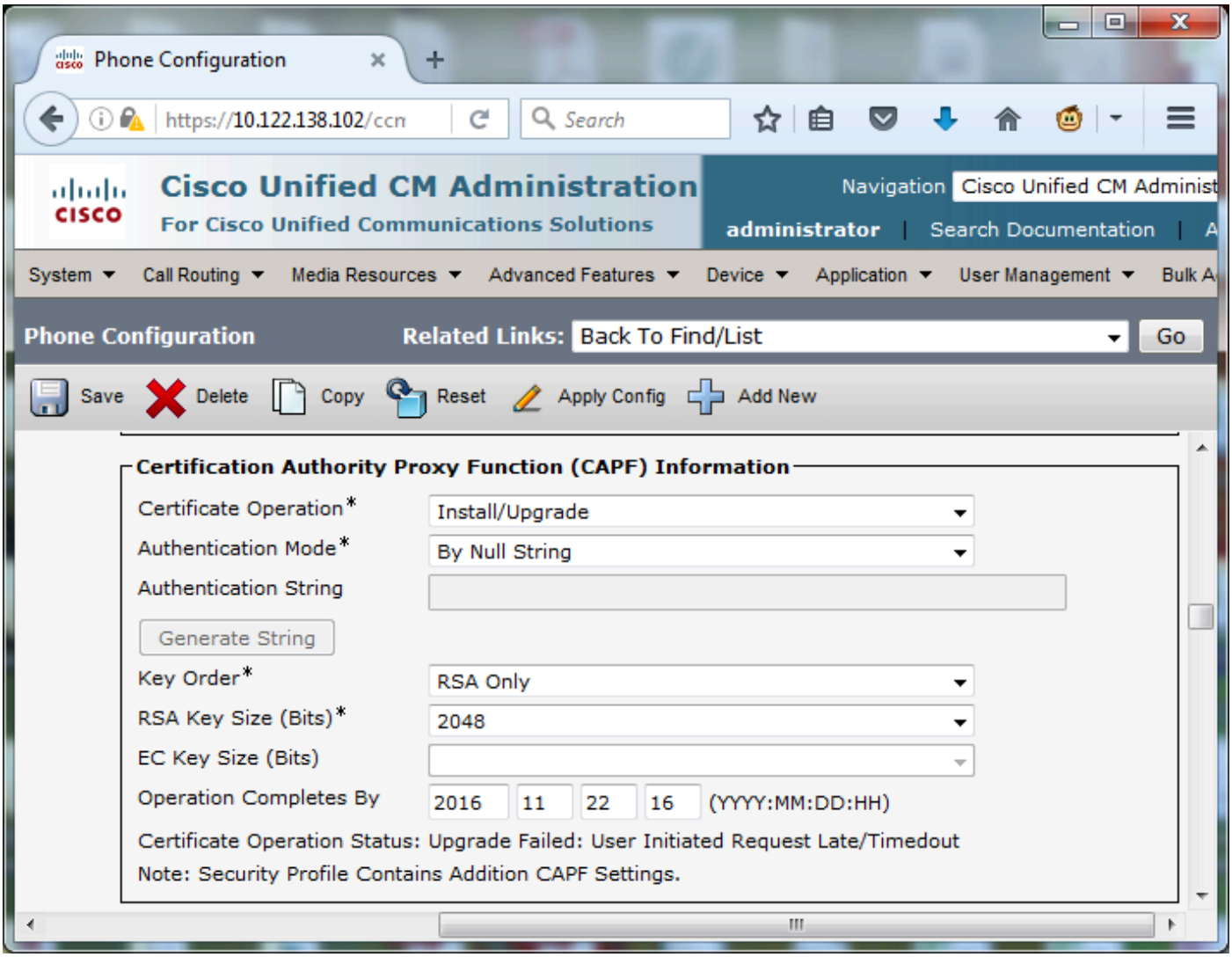
Sur le téléphone, vérifiez qu'un contrôleur LSC n'est pas encore installé, comme illustré dans l'image. Par exemple, sur un téléphone de la gamme 79XX, accédez à Paramètres > 4 - Configuration de la sécurité > 4 - LSC.



Ouvrez la page de configuration de votre téléphone. Accédez à Cisco Unified CM Administration > Device > Phone.

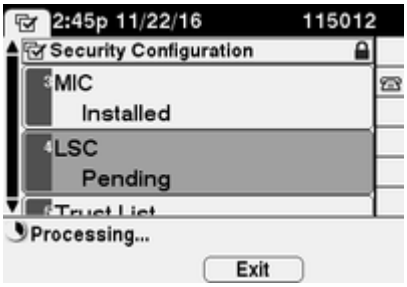
Entrez ces détails dans la section CAPF Information de la configuration du téléphone, comme indiqué dans l'image :

- Pour Certificate Operation, choisissez Install/Upgrade.
- Pour Authentication Mode, choisissez By Null String.
- Pour cet exemple, conservez les valeurs par défaut du système pour l'ordre des clés, la taille de clé RSA (bits) et la taille de clé EC (bits).
- Dans le champ Opération terminée par, entrez une date et une heure ultérieure d'au moins une heure.

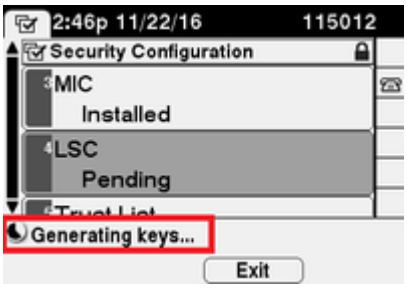


Enregistrez vos modifications de configuration, puis Appliquez la configuration.

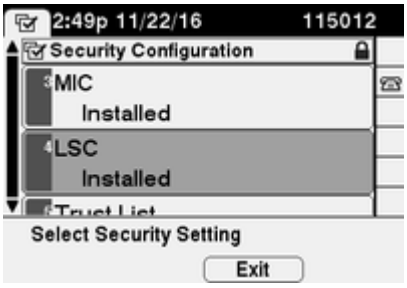
L'état LSC du téléphone passe à En attente, comme indiqué dans l'image.



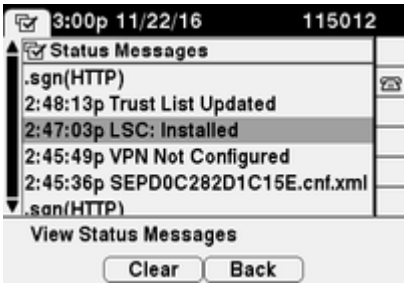
Le téléphone génère des touches comme illustré dans l'image.



Le téléphone se réinitialise et lorsque la réinitialisation est terminée, l'état LSC du téléphone passe à Installé, comme illustré dans l'image.



Elle est également visible sous Messages d'état sur le téléphone, comme illustré dans l'image.



Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Afin de vérifier l'installation du certificat LSC sur plusieurs téléphones, référez-vous à la section Générer un rapport CAPF du Guide de sécurité pour Cisco Unified Communications Manager, version 11.0(1). Vous pouvez également afficher les mêmes données dans l'interface Web Administration de CUCM en utilisant la procédure Find Phones by LSC Status ou Authentication String.

Afin d'obtenir des copies des certificats LSC installés dans les téléphones, référez-vous à l'article Comment récupérer des certificats à partir de téléphones IP Cisco.

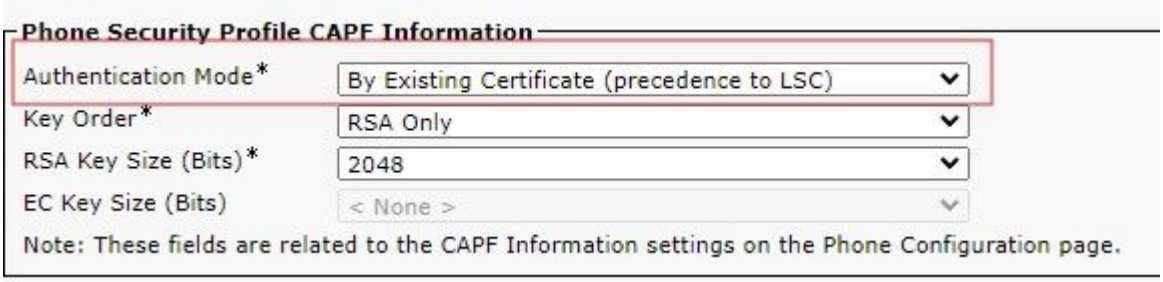
Installation LSC en bloc

Utilisez cette section pour télécharger des LCS en masse vers des téléphones du même modèle.

1. Accédez à Bulk Administration > Phones > Update Phones > Query.
2. Recherchez les téléphones dont le type de périphérique contient <saisissez un numéro de modèle à quatre chiffres>, sélectionnez Rechercher, puis Suivant.
3. Faites défiler jusqu'à la section Informations sur la fonction proxy de l'autorité de certification (CAPF).
4. Dans la section déroulante, sélectionnez Install/Upgrade.

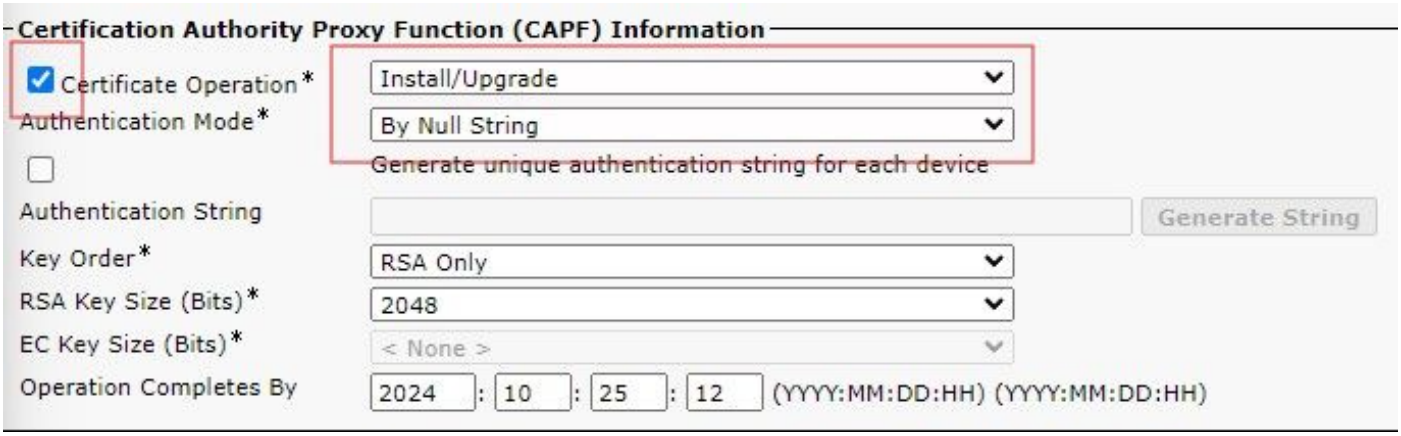
Lorsque vous utilisez l'administration en bloc et que vous sélectionnez le mode d'authentification, ce dernier doit correspondre au fonctionnement du profil de sécurité du téléphone. En cas de non-correspondance, par exemple, Par chaîne Null en masse et Par certificat existant (priorité à LSC) dans le profil de sécurité du téléphone, l'opération ne peut pas se terminer.

Vérifiez le profil de sécurité du téléphone et le mode d'authentification pour vous assurer que vous utilisez le mode correct.



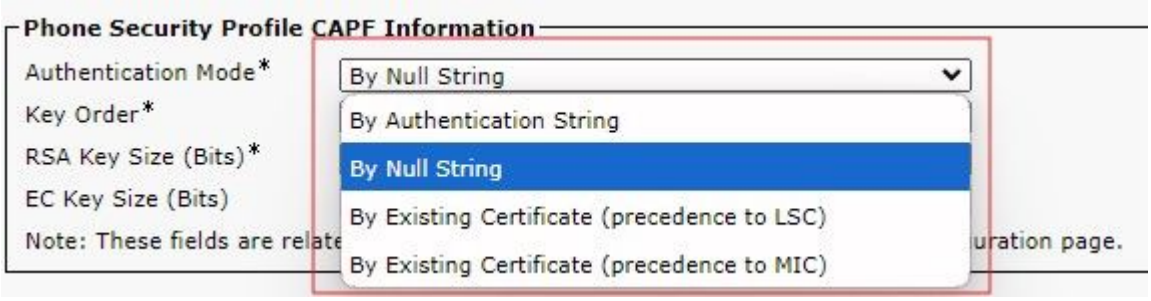
LSC par priorité LSC

Pour définir la configuration en bloc, dans la liste déroulante, sélectionnez le Mode d'authentification qui correspond au profil de sécurité du téléphone.



Sélection en bloc

Si vous modifiez le mode d'authentification du profil de sécurité du téléphone, vous devez enregistrer, puis appliquer la configuration. Cela peut entraîner le redémarrage des périphériques utilisant le profil de sécurité téléphonique spécifique.



Sélection d'authentification

Dépannage

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

Aucun serveur CAPF valide

L'installation du contrôleur LSC échoue. Les messages d'état du téléphone indiquent « No valid CAPF server ». Cela indique qu'il n'y a aucune entrée CAPF dans le fichier ITL. Vérifiez que le service CAPF a été activé, puis redémarrez le service TFTP. Vérifiez que le fichier ITL contient un certificat CAPF après le redémarrage, réinitialisez le téléphone pour récupérer le dernier fichier ITL, puis recommencez l'opération de certificat. Si l'entrée du serveur CAPF dans le menu des paramètres de sécurité du téléphone s'affiche sous la forme d'un nom d'hôte ou d'un nom de domaine complet, vérifiez que le téléphone est en mesure de convertir l'entrée en adresse IP.

LSC : Échec de connexion

L'installation du contrôleur LSC échoue. Les messages d'état du téléphone indiquent « LSC: Échec de la connexion. Cela peut indiquer l'une de ces conditions :

- Non-concordance entre le certificat CAPF dans le fichier ITL et le certificat actuel, le service CAPF est en cours d'utilisation.
- Le service CAPF est arrêté ou désactivé.
- Le téléphone ne peut pas accéder au service CAPF sur le réseau.

Vérifiez que le service CAPF est activé, redémarrez le service CAPF, redémarrez les services TFTP à leur démarrage, réinitialisez le téléphone pour récupérer le dernier fichier ITL, puis recommencez l'opération de certificat. Si le problème persiste, effectuez une capture de paquets à partir du téléphone et du serveur de publication CUCM, puis analysez pour voir s'il existe une communication bidirectionnelle sur le port 3804, le port de service CAPF par défaut. Sinon, il peut y avoir un problème de réseau.

LSC : Échec

L'installation du contrôleur LSC échoue. Les messages d'état du téléphone indiquent « LSC: Échec ». La page Web Configuration du téléphone affiche « État de l'opération de certificat : Échec de la mise à niveau : Requête initiée par l'utilisateur tardive/expirée". Cela indique que la date et l'heure de fin de l'opération ont expiré ou sont passées. Entrez une date et une heure futures d'au moins une heure, puis recommencez l'opération de certificat.

LSC : Opération en attente

L'installation du contrôleur LSC échoue. Les messages d'état du téléphone indiquent « LSC: Échec de la connexion. La page de configuration du téléphone affiche « État de l'opération de certificat : Opération en attente". Il y a différentes raisons pour lesquelles on peut voir l'état de l'opération de certificat : État Opération en attente. Voici quelques-unes d'entre elles :

- ITL sur le téléphone est différent de celui actuellement utilisé sur les serveurs TFTP configurés.
- Problèmes avec des ITL corrompus. Dans ce cas, les périphériques perdent leur état de confiance et la commande utils itl reset localkey doit être exécutée à partir du serveur de publication CUCM pour forcer les téléphones à utiliser maintenant le certificat ITLRecovery. Si le cluster est en mode mixte, vous devez utiliser la commande utils ctl reset localkey. Ensuite, vous voyez un exemple de ce que vous pouvez voir lorsque vous essayez d'afficher un ITL corrompu à partir de l'interface de ligne de commande de CUCM. S'il y a une erreur quand vous essayez d'afficher l'ITL et essayez d'exécuter la commande utils itl reset localkey, mais que vous voyez la deuxième erreur, il peut s'agir d'un défaut de l'ID de bogue Cisco CSCus3755. Confirmez si la version du CUCM est affectée.

```
admin:show itl
Length of ITL file: 0
ITL File not found. To generate an ITL file, activate or restart the Cisco TFTP service as this command is only valid on tftp
servers.
Error parsing the ITL File.
```

```
admin:utils itl reset localkey
Enter CCM Administrator password :

Locating active Tftp servers in the cluster.....

Unable to determine the active and running  TFTP nodes in the cluster
Ensure that the DB replication is working on all nodes and the correct Password has been entered
Then retry the command

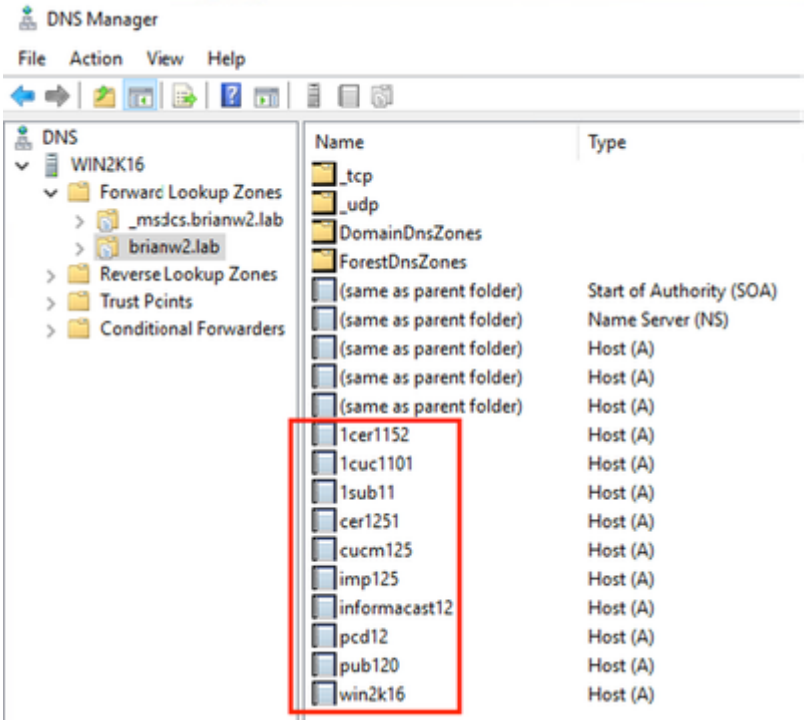
Executed command unsuccessfully
chmod: changing permissions of `/var/log/active/cm/trace/dbl/sdi/replication_scripts_output.log': Operation not permitted
```

- Le téléphone ne parvient pas à authentifier le nouveau LSC en raison d'une défaillance du TVS.
- Le téléphone utilise le certificat MIC, mais la section Certificate Authority Proxy Function (CAPF) Information de la page de configuration des téléphones a le mode d'authentification défini sur par le certificat existant (priorité à LSC).
- Le téléphone ne peut pas résoudre le nom de domaine complet de CUCM.

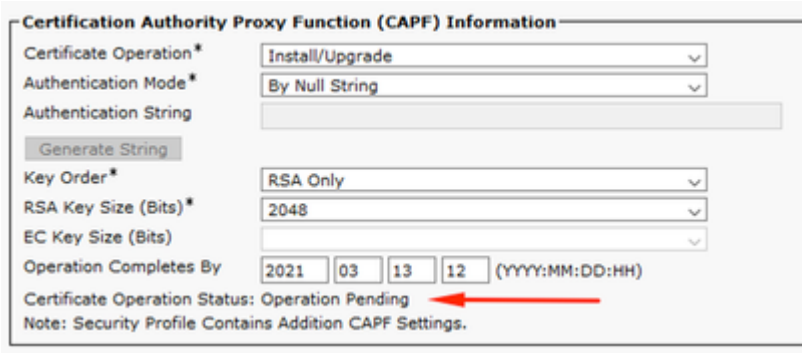
Pour le dernier scénario, un environnement de travaux pratiques est configuré pour simuler ce que vous verriez dans les journaux si un téléphone n'était pas en mesure de résoudre le nom de domaine complet de CUCM. Actuellement, les travaux pratiques sont configurés avec les serveurs suivants :

- Éditeur et abonné CUCM exécutant la version 11.5.1.15038-2
- Configuration de Windows 2016 Server en tant que serveur DNS

Pour le test, aucune entrée DNS n'est configurée pour le serveur PUB11 CUCM.



Tentative de transmission d'un LSC à l'un des téléphones (8845) du TP. Vérifiez qu'il affiche toujours l'état d'opération du certificat : Opération en attente.



Dans les journaux de la console téléphonique, vérifiez que le téléphone tente d'interroger son cache local (127.0.0.1) avant de transférer la requête à l'adresse du serveur DNS configurée.

```
0475 INF Mar 12 15:07:53.686410 dnsmasq[12864]: query[A] PUB11.brianw2.lab from 127.0.0.1
0476 INF Mar 12 15:07:53.686450 dnsmasq[12864]: forwarded PUB11.brianw2.lab to X.X.X.X
0477 INF Mar 12 15:07:53.694909 dnsmasq[12864]: forwarded PUB11.brianw2.lab to X.X.X.X
0478 INF Mar 12 15:07:53.695263 dnsmasq[12864]: reply PUB11.brianw2.lab is NXDOMAIN-IPv4
0479 INF Mar 12 15:07:53.695833 dnsmasq[12864]: query[A] PUB11.brianw2.lab from 127.0.0.1
0480 INF Mar 12 15:07:53.695865 dnsmasq[12864]: cached PUB11.brianw2.lab is NXDOMAIN-IPv4
0481 WRN Mar 12 15:07:53.697091 (12905:13036) JAVA-configmgr MQThread|NetUtil.traceIPv4DNSErrors:? - DN

++ However, we see that the phone is not able to resolve the FQDN of the CUCM Publisher. This is becaus

0482 ERR Mar 12 15:07:53.697267 (12905:13036) JAVA-configmgr MQThread|cip.sec.TvsProperty:? - Failed to

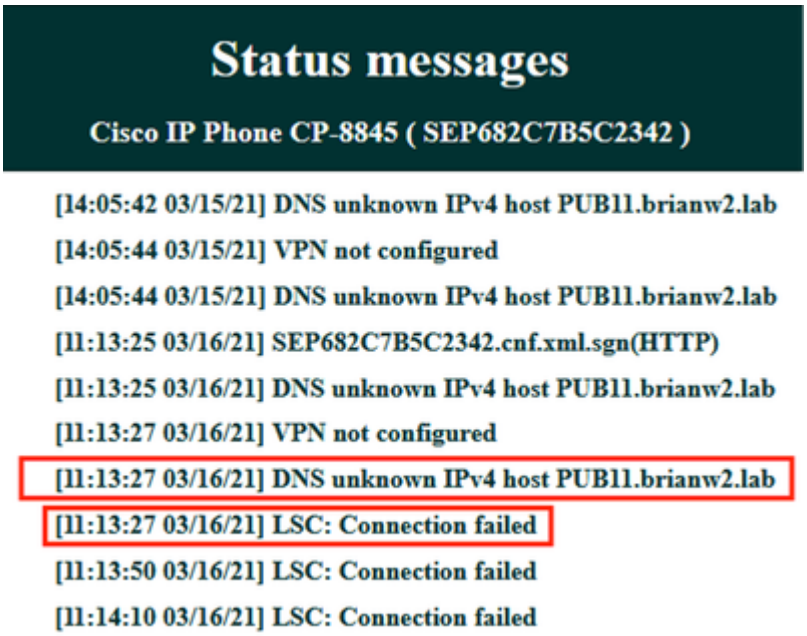
++ Afterwards, we see the CAPF operation fail. This is expected because we do not have a DNS mapping fo

0632 NOT Mar 12 15:07:55.760715 (12905:13036) JAVA-configmgr MQThread|cip.sec.CertificateProperty:? - C
0633 NOT Mar 12 15:07:55.761649 (322:17812) SECUREAPP-RCAPF_START_MODE: Start CAPF - mode:[1]([NULL_STR
0634 NOT Mar 12 15:07:55.761749 (322:17812) SECUREAPP-CAPF_CLNT_INIT:CAPF clnt initialized
0635 NOT Mar 12 15:07:55.761808 (322:17812) SECUREAPP-CAPFClnt: SetDelayTimer - set with value <0>
0636 ERR Mar 12 15:07:55.761903 (322:17812) SECUREAPP-Sec create BIO - invalid parameter.
0637 ERR Mar 12 15:07:55.761984 (322:17812) SECUREAPP-SEC_CAPF_BIO_F: CAPF create bio failed
0638 ERR Mar 12 15:07:55.762040 (322:17812) SECUREAPP-SEC_CAPF_OP_F: CAPF operation failed, ret -7
0639 CRT Mar 12 15:07:55.863826 (12905:13036) JAVA-configmgr MQThread|cip.sec.CertificateProperty$1:? -

++ What we would expect to see is something similar to the following where DNS replies with the IP addr

4288 INF Mar 12 16:34:06.162666 dnsmasq[12864]: query[A] PUB11.brianw2.lab from 127.0.0.1
4289 INF Mar 12 16:34:06.162826 dnsmasq[12864]: forwarded PUB11.brianw2.lab to X.X.X.X
4290 INF Mar 12 16:34:06.164908 dnsmasq[12864]: reply PUB11.brianw2.lab is X.X.X.X
4291 NOT Mar 12 16:34:06.165024 (12905:13036) JAVA-configmgr MQThread|cip.sec.TvsProperty:? - Resolve T
```

Reportez-vous aux messages d'état du téléphone indiquant que le téléphone n'est pas en mesure de résoudre PUB11.brianw2.lab. Reportez-vous ensuite à la section « LSC: Message d'échec de la connexion.



Défauts à prendre en compte :

ID de bogue Cisco CSCub62243 - L'installation de LSC échoue par intermittence, puis le serveur CAPF est gelé.

Défaut d'amélioration à prendre en compte :

ID de bogue Cisco CSCuz18034 - Rapport nécessaire pour les terminaux LSC installés, ainsi que l'état d'expiration.

Informations connexes

Ces documents fournissent plus d'informations sur l'utilisation des LSC dans le contexte de l'authentification client VPN AnyConnect et de l'authentification 802.1X.

- Téléphone VPN AnyConnect - Dépannage des téléphones IP, ASA et CUCM
- Services de mise en réseau basés sur l'identité : Guide de déploiement et de configuration de la téléphonie IP dans les réseaux compatibles IEEE 802.1X

Il existe également un type avancé de configuration LSC, dans lequel les certificats LSC sont signés directement par une autorité de certification tierce, et non le certificat CAPF.

Pour plus de détails, référez-vous à : Exemple de configuration de génération et d'importation de LSC signés par une autorité de certification tierce CUCM

- Assistance et documentation techniques - Cisco Systems

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.