Configurez le LSC sur le téléphone IP de Cisco avec CUCM

Contenu

Introduction

Ce document décrit comment installer le certificat significatif a localement - (LSC) à un téléphone d'Internet Protocol de Cisco (téléphone IP de Cisco).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Options de security mode de batterie de Cisco Unified Communications Manager (CUCM)
- Certificats X.509
- Certificats installés de fabrication (MICs)
- LSC
- Exécutions de certificat de la fonction de proxy d'autorité de certification (CAPF)
- Sécurité par défaut (SBD)
- Fichiers initiaux de la liste de confiance (ITL)

[Composants utilisés](#)

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

Note: Il concerne également seulement les téléphones qui prennent en charge le SBD. Par exemple, les 7940 et 7960 téléphones ne prennent en charge pas le SBD, ni font 7936 et 7937 téléphones de conférence les 7935. Pour une liste de périphériques qui prennent en charge le SBD dans votre version de CUCM, naviguez vers **Cisco Unified signalant > système signale > liste de caractéristique de téléphone d'Unified CM** et exécute un état sur la **caractéristique : Sécurité par défaut**.

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.

Informations générales

MICs contre des LSC

Si vous utilisez l'authentification basée par certificat pour le 802.1X ou le téléphone VPN d'Anyconnect, il est important de comprendre la différence entre MICs et LSC.

Chaque téléphone Cisco est livré avec une MIC préinstallée à l'usine. Ce certificat est signé par un de Cisco fabriquant des Certificats CA, de Cisco fabriquant le CA, de Cisco fabriquant le certificat SHA2, CAP-RTP-001 ou CAP-RTP-002 CA. Quand le téléphone présente ce certificat, il montre que c'est un téléphone Cisco valide, mais ceci ne valide pas que le téléphone appartient à un client spécifique ou à la batterie CUCM. C'a pu potentiellement être un téléphone escroc acheté sur le marché libre ou apporté plus d'un site différent.

Des LSC, d'autre part, sont intentionnellement installés aux téléphones par un administrateur, et sont signés par le certificat CAPF CUCM Publisher. Vous configureriez le 802.1X ou l'Anyconnect VPN pour faire confiance seulement à des LSC émis par les autorités de certification connues CAPF. Baser l'authentification de certificat sur des LSC au lieu de MICs te fournit un contrôle beaucoup plus granulaire au-dessus duquel les appareils téléphoniques sont de confiance.

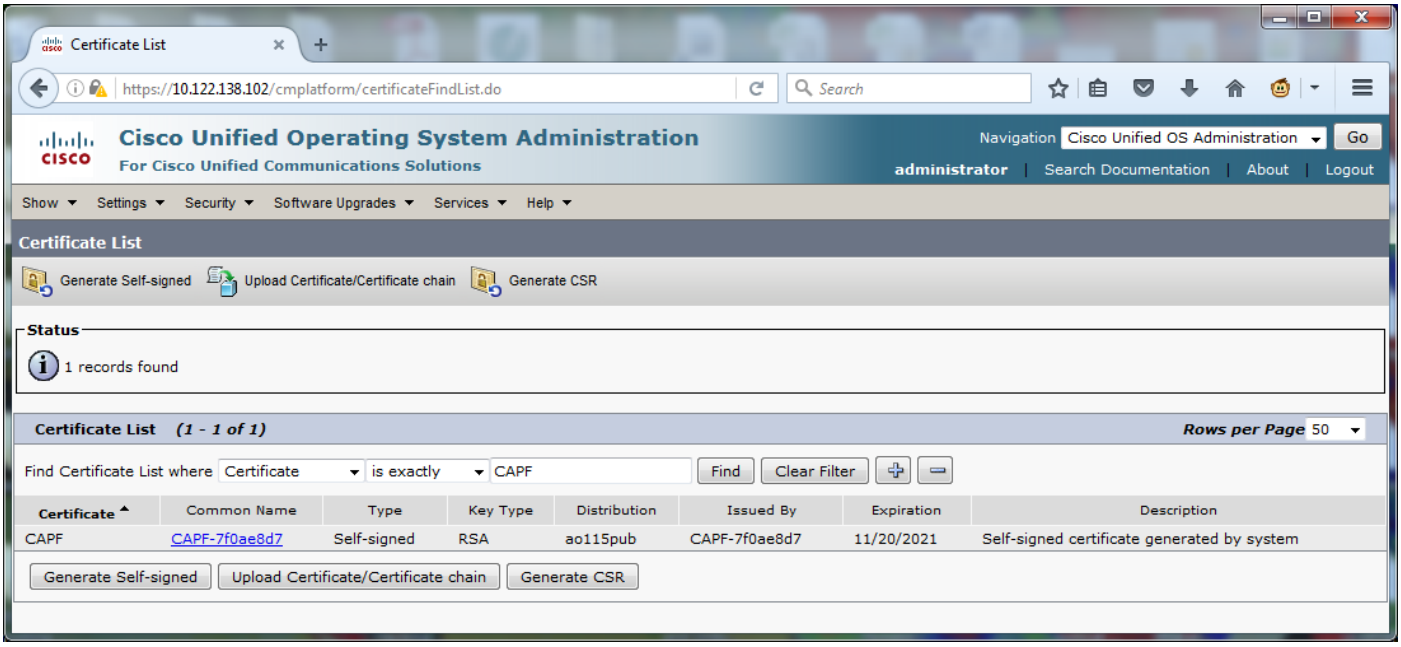
Configurez

Topologie du réseau

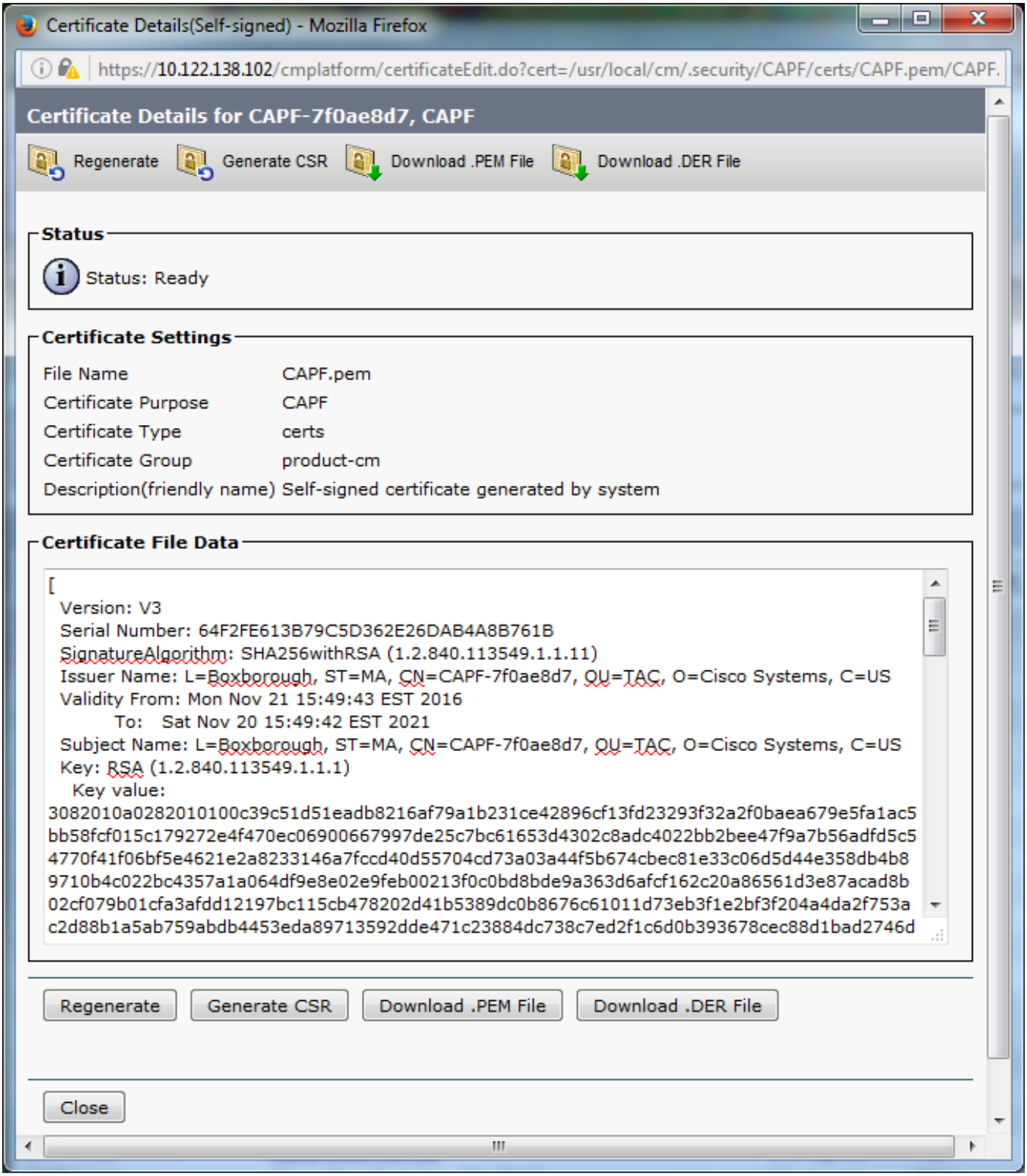
Ces serveurs de laboratoire CUCM ont été utilisés pour ce document :

- ao115pub - 10.122.138.102 - serveur CUCM Publisher et TFTP
- ao115sub - 10.122.138.103 - abonné CUCM et serveur TFTP

Vérifiez que le certificat CAPF n'a pas expiré, ni est environ expirer dans un avenir proche. Naviguez vers la **gestion de SYSTÈME D'EXPLOITATION de Cisco Unified > la Gestion de Sécurité > de certificat**, puis la **liste de certificat de découverte où le certificat est exactement CAPF** suivant les indications de l'image.



Cliquez sur le **nom commun** afin d'ouvrir la page de détails de certificat. Examinez la validité **de :** et **à :** dates dans le volet de **données de fichier du certificat** afin de déterminer quand le certificat expire, suivant les indications de l'image.



Si le certificat CAPF a expiré, ou est bientôt d'expirer, régénérer ce certificat. N'avancez pas avec le LSC installent le processus avec expirée ou bientôt expirez certificat CAPF. Ceci évite la nécessité de réviser des LSC dans un avenir proche dus à l'expiration de certificat CAPF. Pour des informations sur la façon régénérer le certificat CAPF, référez-vous l'article de régénération de certificat CUCM/processus de renouvellement.

De même, si vous devez faire signer votre certificat CAPF par une autorité de certification de tiers, vous avez un choix à faire à ce stade. Terminez-vous la génération de fichier de la demande de signature de certificat (CSR) et l'importation du certificat signé CAPF maintenant, ou continuez la configuration avec un LSC auto-signé pour un test préliminaire. Si vous avez besoin d'un certificat CAPF signé par tiers, il est généralement raisonnable pour configurer cette caractéristique d'abord

avec un certificat auto-signé CAPF, test et pour la vérifier, et redéploie alors les LSC qui sont signés par un certificat CAPF signé par tiers. Ceci simplifie le dépannage postérieur, si les tests avec le certificat CAPF signé par tiers échouent.

> **Avertissement** : Si vous régénérez le certificat CAPF ou importez un certificat CAPF signé par tierce partie tandis que le service CAPF est lancé et commencé, des téléphones sont automatiquement remis à l'état initial par CUCM. Remplissez ces procédures dans une fenêtre de maintenance quand il est acceptable que des téléphones soient remis à l'état initial. Pour la référence, voir le CSCue55353 - Ajoutez l'avertissement en régénérant le certificat TVS/CCM/CAPF ce téléphone la remise.

> **Note**: Si votre version CUCM prend en charge le SBD, cette procédure d'installation LSC s'applique sans se soucier si votre batterie CUCM est placée au mode mixte ou pas. Le SBD est une partie de version 8.0(1) et ultérieures CUCM. Dans ces versions de CUCM, les fichiers ITL contient le certificat pour le service CAPF sur le CUCM Publisher. Ceci permet à des téléphones pour se connecter au service CAPF afin de prendre en charge des exécutions de certificat comme installent/mises à jour et dépannent.

> Dans les versions préalables de CUCM, il était nécessaire de configurer la batterie pour le mode mixte afin de prendre en charge des exécutions de certificat. Car ce n'est plus nécessaire, ceci ramène des barrières à l'utilisation des LSC comme certificats d'identité de téléphone pour l'authentification de 802.1X ou pour l'authentification de client vpn d'AnyConnect.

Exécutez la commande **ITL d'exposition** sur tous les serveurs TFTP dans la batterie CUCM. Observez que le fichier ITL fait contient un certificat CAPF.

Par exemple, voici un extrait de l'**ITL d'exposition** sortie de l'abonné ao115sub du laboratoire CUCM.

> **Note**: Il y a une entrée record ITL dans ce fichier avec une FONCTION de CAPF.

> **Note**: Si votre fichier ITL n'a pas une entrée CAPF, ouvre une session à votre éditeur CUCM et la confirme le service CAPF est lancé. Afin de confirmer ceci, naviguez vers le **Serviceability > Tools > Service Activation > le CUCM Publisher > Sécurité de Cisco Unified**, puis lancez le **service de fonction de proxy d'autorité de certification de Cisco**. Si le service était désactivé et vous le lanciez juste, naviguez vers l'**utilité > le Tools > Control Center de Cisco Unified – comportez les services > le serveur > les services cm**, alors redémarrez le service TFTP de Cisco sur tous les serveurs TFTP dans la batterie CUCM pour régénérer le fichier ITL. En outre, assurez-vous que vous ne frappez pas CSCuj78330.

> **Note**: Après que vous soyez fait, exécutez la commande **ITL d'exposition** sur tous les serveurs TFTP dans la batterie CUCM afin de vérifier que le certificat du courant CUCM Publisher CAPF est maintenant inclus dans le fichier.

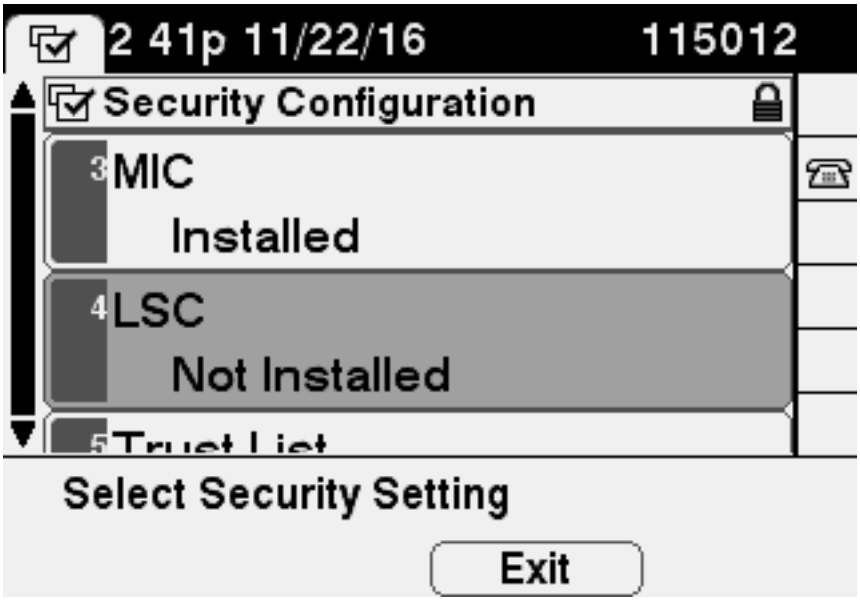
```
 ITL Record #:1
 ----
BYTEPOS TAG LENGTH VALUE
```

```
------- --- ------ -----
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.
```

L'entrée CAPF étant confirmé comme entrée dans l'ITL, vous pouvez se terminer une exécution de certificat à un téléphone. Dans cet exemple, un certificat de 2048 bits RSA est installé au moyen de l'authentification de chaîne null.

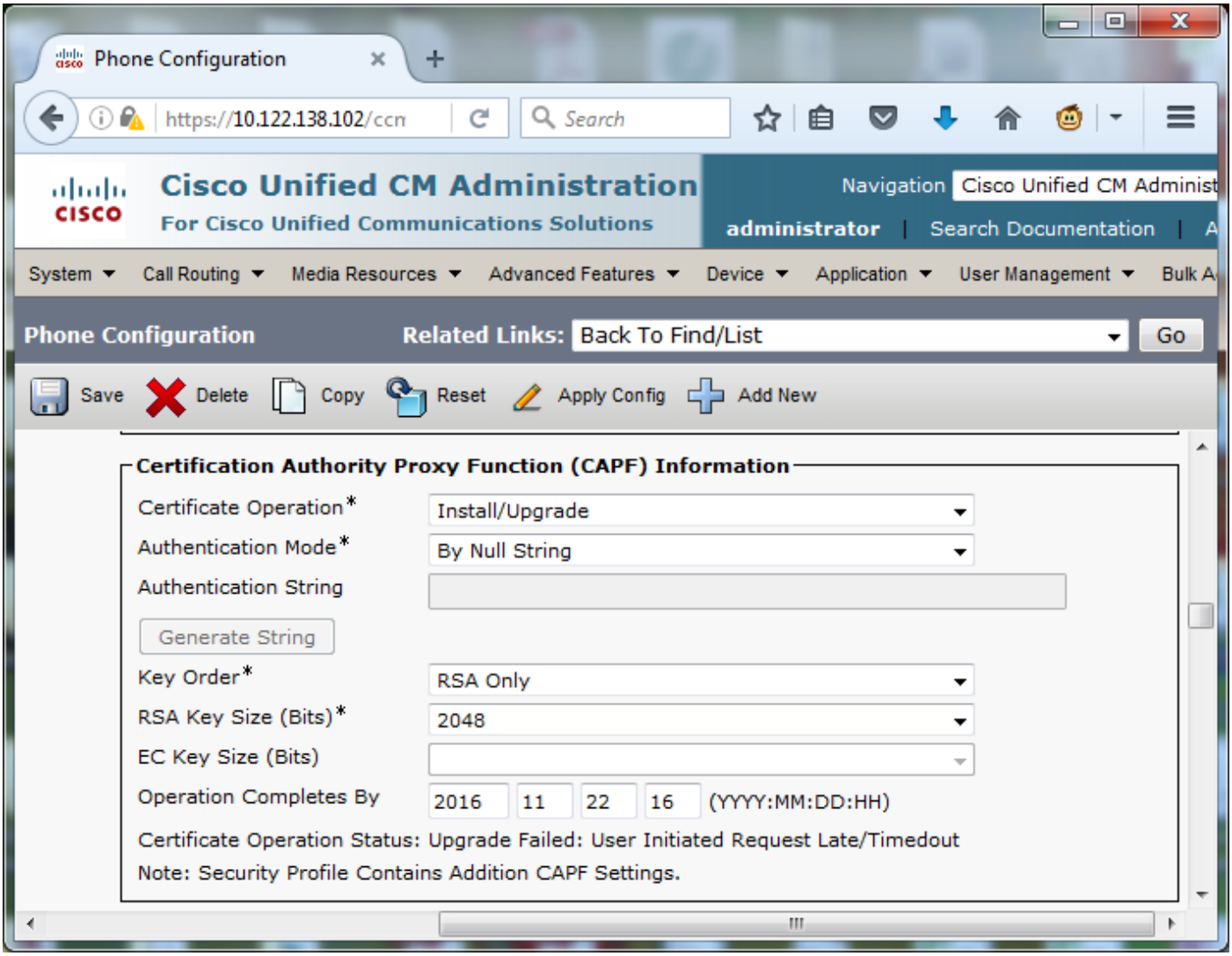
Au téléphone, vérifiez qu'un LSC n'est pas encore installé suivant les indications de l'image. Par exemple, sur un 79XX la gamme téléphone, navigue vers des **configurations > 4 - configuration de sécurité > 4 - LSC**.



Ouvrez la page de configuration de téléphone pour votre téléphone. Naviguez vers la **gestion > le Device > Phone de Cisco Unified CM**.

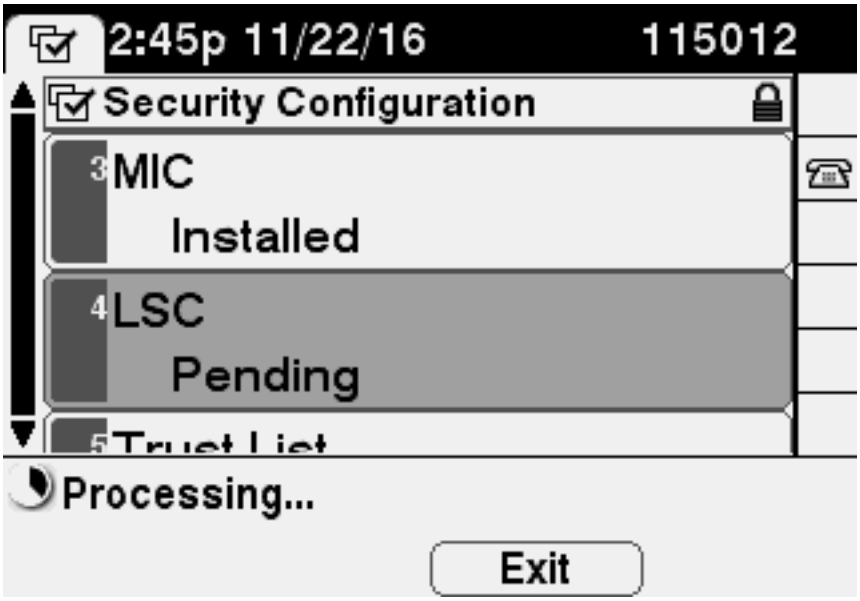
Écrivez ces détails à la section Informations CAPF de la configuration du téléphone, suivant les indications de l'image :

- Pour l'exécution de certificat, choisi **installez/mise à jour**
- Pour l'authentication mode, sélectionnez **par la chaîne null**
- Pour cet exemple, laissez la commande, la taille principales de clé RSA (bits) et la taille de clé EC (bits) a placé aux **paramètres systèmes par défaut**.
- Pour l'exécution se termine par, écrit une date et une heure qui est au moins d'une heure dedans au futur.

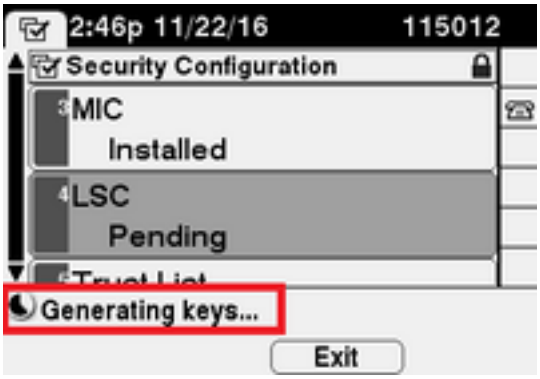


Sauvegardez vos modifications de configuration, puis **appliquez le config**.

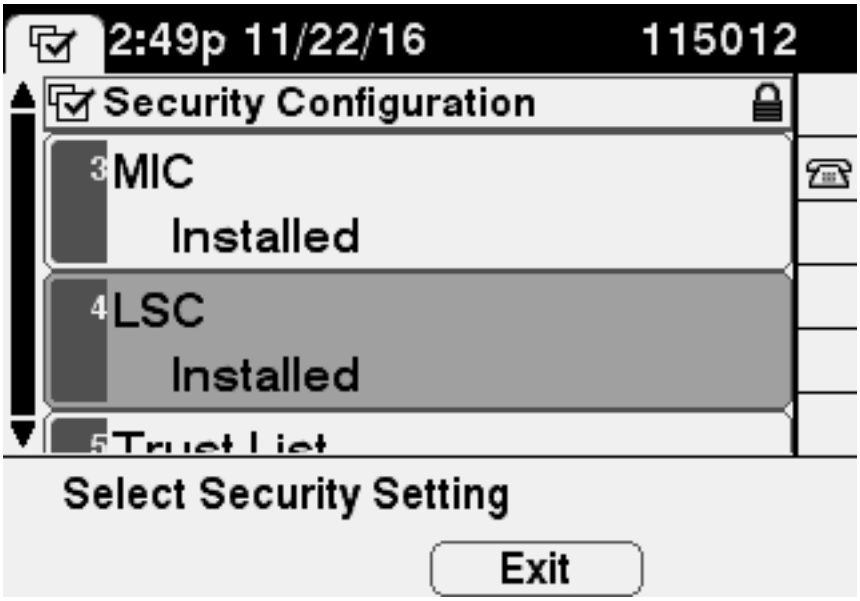
L'état LSC au téléphone change à **en suspens** suivant les indications de l'image.



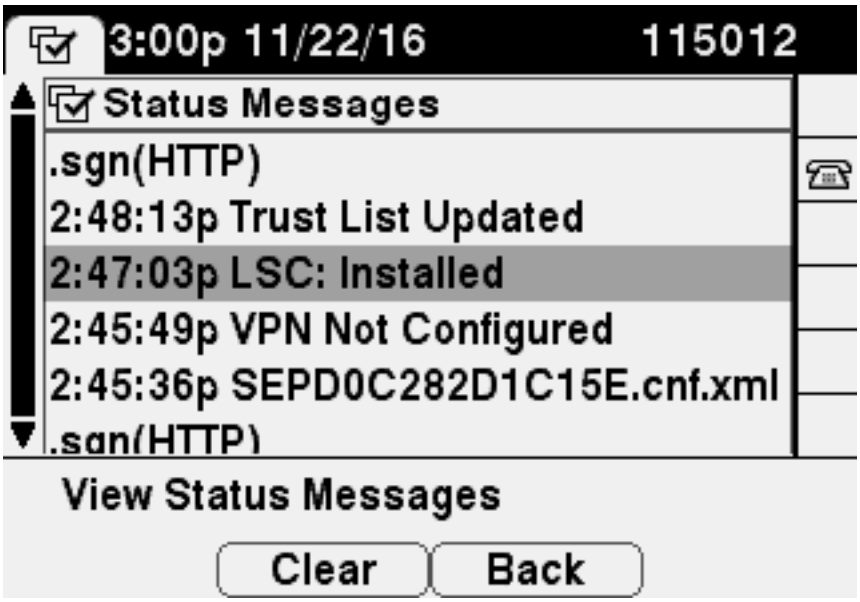
Le téléphone génère des clés suivant les indications de l'image.



Les remises de téléphone, et quand la remise se termine, les changements d'état du téléphone LSC à **installé** suivant les indications de l'image.



C'est également les **messages** de dessous visibles d'**état** dans le téléphone suivant les indications de l'image.



Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Afin de vérifier l'installation de certificat LSC à de plusieurs téléphones, référez-vous la section d'état du générer CAPF du guide de Sécurité pour Cisco Unified Communications Manager, la version 11.0(1). Alternativement, vous pouvez visualiser les mêmes données dans l'interface web de gestion CUCM au moyen des téléphones de découverte par procédure d'état ou de chaîne d'authentification LSC.

Afin d'obtenir des copies des Certificats LSC installés dans des téléphones, référez-vous le comment récupérer des Certificats du phonesarticle IP de Cisco.

Dépannez

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

Aucun serveur valide CAPF

Le LSC n'installe pas. Les messages de l'état du téléphone n'affichent **aucun serveur valide CAPF**. Ceci indique qu'il n'y a aucune entrée CAPF dans le fichier ITL. Vérifiez que le service CAPF a été lancé, et puis redémarrez le service TFTP. Vérifiez que le fichier ITL contient un certificat CAPF après que la reprise, ait remis à l'état initial le téléphone pour prendre le dernier fichier ITL, et puis relance votre exécution de certificat. Si l'entrée de serveur CAPF dans les affichages de menu des paramètres de sécurité du téléphone comme adresse Internet ou nom de domaine complet, confirment le téléphone peut résoudre l'entrée à une adresse IP.

LSC : La connexion a manqué

Le LSC n'installe pas. L'exposition **LSC de** messages de l'état du téléphone **: La connexion a manqué**. Ceci peut indiquer une de ces conditions :

- Une non-concordance entre le certificat CAPF dans le fichier ITL et le certificat valable, le service CAPF est en service.
- Le service CAPF est arrêté ou désactivé.
- Le téléphone ne peut pas atteindre le service CAPF au-dessus du réseau.

Vérifiez le service CAPF est lancé, redémarre le service CAPF, clusterwide de services TFTP de reprise, remet à l'état initial le téléphone pour prendre le dernier fichier ITL, et puis relance votre exécution de certificat. Si le problème persiste, prenez une capture de paquet du téléphone et du CUCM Publisher, et l'analysez afin de voir s'il y a transmission bidirectionnelle sur le port 3804, le port de service du par défaut CAPF. Sinon, il peut y a un problème de réseau.

LSC : Manqué

Le LSC n'installe pas. L'exposition **LSC de** messages de l'état du téléphone **: Manqué**. **L'état d'exécution de certificat d'**expositions de page Web de configuration de téléphone **: La mise à jour a manqué : Tard de demande initié par utilisateur/Timedout**. Ceci indique que l'exécution se termine par date et heure ont expiré ou ont lieu dans le passé. Écrivez une date et une heure qui est au moins d'une heure dedans au futur, et puis relancez votre exécution de certificat.

Informations connexes

Ces documents fournissent plus d'informations sur l'utilisation des LSC dans le contexte pour

l'authentification de client vpn d'AnyConnect et l'authentification de 802.1X.

- Téléphone d'AnyConnect VPN - Téléphones IP, dépannage ASA, et CUCM
- Services basés sur identité de réseau : Téléphonie sur IP dans le déploiement et le guide de configuration de réseaux d'IEEE 802.1X-Enabled

Il y a également un type avancé de configuration LSC, dans lequel les Certificats LSC sont signés directement par une autorité de certification de tiers, pas le certificat CAPF.

Pour des détails, référez-vous : Exemple de configuration de génération Ca-signé par tierce partie et d'importation CUCM LSC

- Support et documentation techniques - Cisco Systems