LSC op IP-telefoon configureren met CUCM

Inhoud

Inleiding

Dit document beschrijft hoe u een Lokaal significant certificaat (LSC) kunt installeren op een Cisco Internet Protocol-telefoon (Cisco IP-telefoon).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Unified Communications Manager (CUCM) Cluster Security Mode-opties
- X.509-certificaten
- Geïnstalleerde certificaten voor productieomgevingen (MICâ€™s)
- LSCâ€™s
- Certificaatverleningsfunctie (CAPF)
- Standaard beveiliging (SBD)
- Initial Trust List (ITL) bestanden

Gebruikte componenten

De informatie in dit document is gebaseerd op CUCM-versies die SBD ondersteunen, namelijk CUCM 8.0(1) en hoger.

> **Opmerking**: het is alleen van toepassing op telefoons die Security By Default (SBD) ondersteunen. De 7940 en 7960 telefoons ondersteunen bijvoorbeeld geen SBD, noch de 7935, 7936 en 7937 vergadertelefoons. Voor een lijst van apparaten die SBD in uw versie van CUCM steunen, navigeer aan **Cisco Unified Reporting > Systeemrapporten > Unified CM Phone Functielijst** en voer een rapport uit over Functie: Beveiliging op standaard.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

MIC's versus LSC's

Als u voor 802.1X of AnyConnect Phone VPN op basis van certificaten gebruikt, is het belangrijk om het verschil tussen MICâ€™s en LSCâ€™s te begrijpen.

Elke Cisco-telefoon wordt geleverd met een vooraf in de fabriek geïnstalleerde MIC. Dit certificaat wordt ondertekend door een van de Cisco Manufacturing CA-certificaten, hetzij door Cisco Manufacturing CA, Cisco Manufacturing CA SHA2, CAP-RTP-001 of CAP-RTP-002 certificaat. Wanneer de telefoon dit certificaat voorlegt, bewijst het dat het een geldige telefoon van Cisco is, maar dit bevestigt niet dat de telefoon tot een specifieke klant of een cluster CUCM behoort. Het kan een schurkentelefoon zijn die op de open markt wordt gekocht of van een andere site wordt overgenomen.

LSCâ€™s daarentegen worden opzettelijk geïnstalleerd op telefoons door een beheerder en worden ondertekend door het CAPF-certificaat van de CUCM Publisher. U zou 802.1X of AnyConnect VPN configureren om alleen LSCâ€™s te vertrouwen die worden verstrekt door bekende CAPF-certificeringsinstanties. Het baseren van certificaatauthentificatie op LSCs in plaats van MICs voorziet u van een veel meer korrelige controle waarover telefoonapparaten worden vertrouwd op.

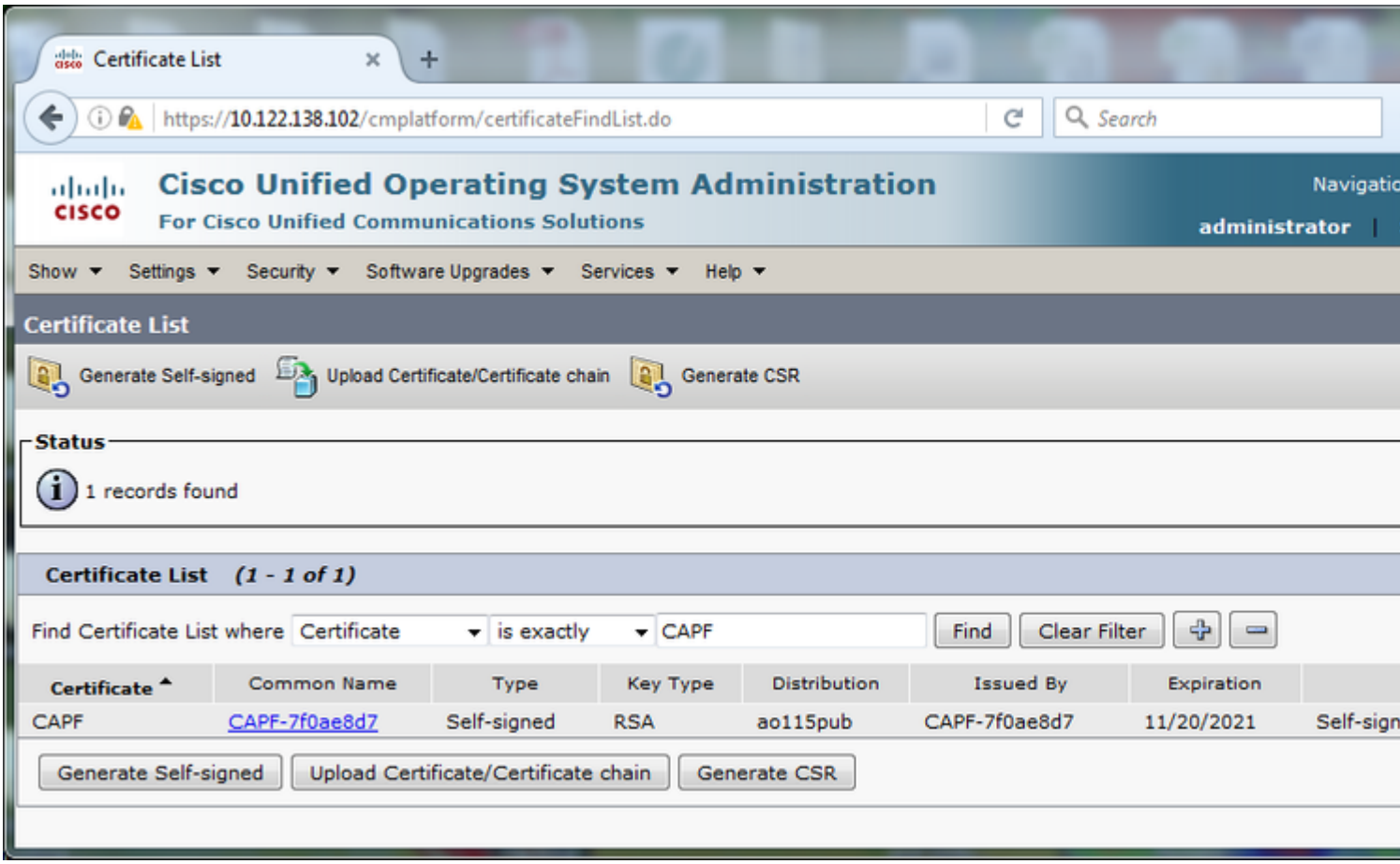
Configureren

Netwerktopologie

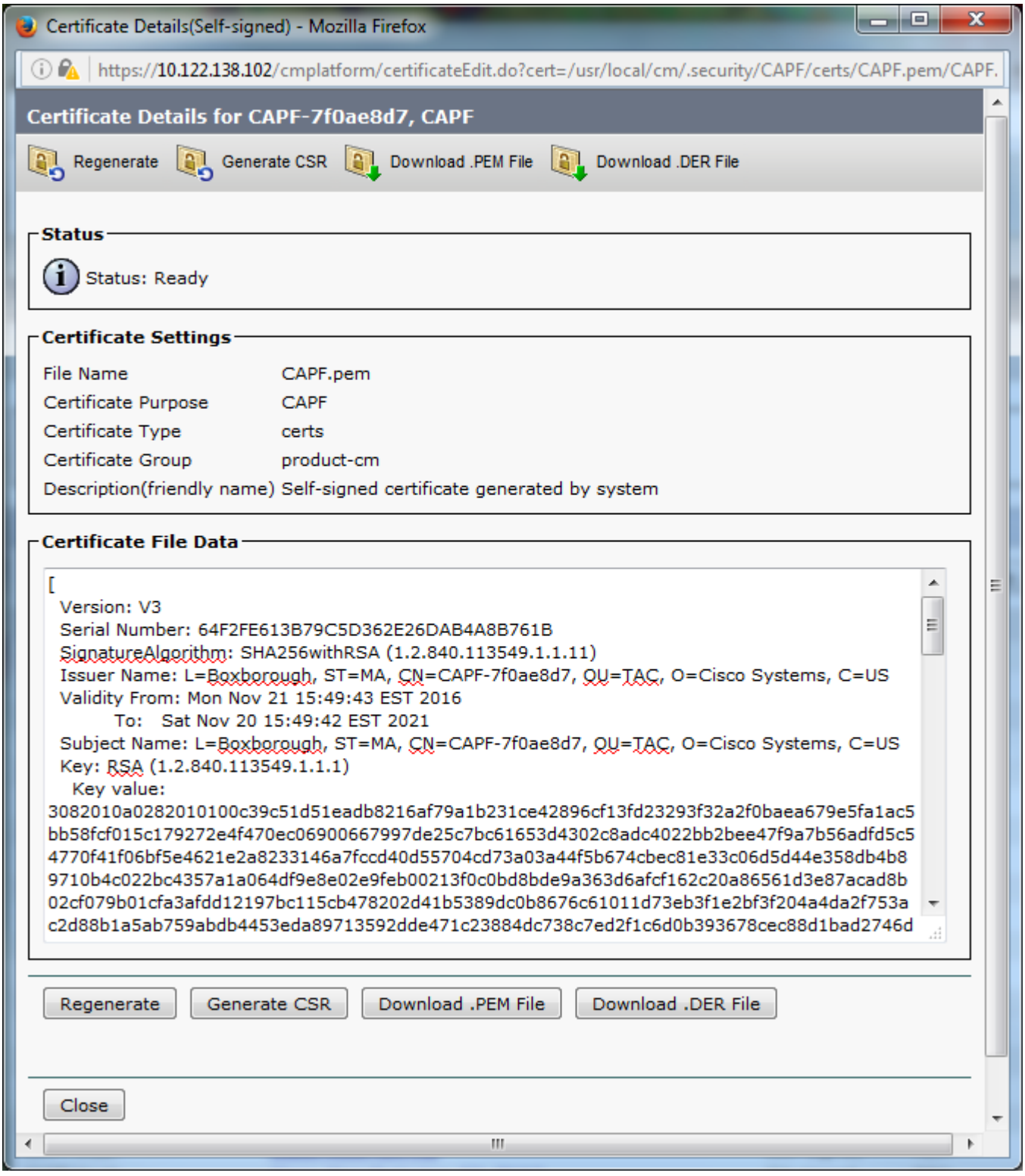
Deze CUCM-laboratoriumservers zijn voor dit document gebruikt:

- ao115pub - 10.122.138.102 - CUCM Publisher & TFTP server
- ao115sub - 10.122.138.103 - CUCM Subscriber & TFTP-server

Controleer of het CAPF-certificaat niet is verlopen of in de nabije toekomst op het punt staat te verlopen. Navigeer naar **Cisco Unified OS-beheer > Beveiliging > certificaatbeheer** en **vind** vervolgens **de certificaatlijst met certificaten waar het certificaat precies CAPF is,** zoals in de afbeelding.



Klik op **algemene naam** om de pagina Certificaatdetails te openen. Inspecteer de geldigheid van: en tot: datums in het deelvenster **certificaatbestandsgegevens** om te bepalen wanneer het certificaat verloopt, zoals in de afbeelding.



Als het CAPF-certificaat is verlopen of binnenkort verloopt, moet u dat certificaat regenereren. Ga niet verder met het LSC-installatieproces met een verlopen of binnenkort verlopen CAPF-certificaat. Dit vermijdt de noodzaak om LSCâ€™s in de nabije toekomst opnieuw uit te geven vanwege het verlopen van het CAPF-certificaat. Raadpleeg voor informatie over het regenereren van het CAPF-certificaat het artikel CUCM-certificaatregeneratie/vernieuwingsproces.

Evenzo, als u uw CAPF certificaat moet laten ondertekenen door een derde partij Certificaatautoriteit, hebt u in dit stadium een keuze te maken. Voltooi ofwel nu het genereren en importeren van het ondertekende CAPF-certificaat van het CSR-bestand (Certificate Signing request), ofwel ga door met de configuratie met een zelf-ondertekende LSC voor een voorlopige test. Als u een door derden ondertekend CAPF-certificaat nodig hebt, is het over het algemeen verstandig om deze optie eerst te configureren met een zelf ondertekend

CAPF-certificaat, te testen en te verifiëren en vervolgens LSCâ€™s opnieuw te implementeren die zijn ondertekend door een door derden ondertekend CAPF-certificaat. Dit vereenvoudigt latere probleemoplossing, als tests met het door derden ondertekende CAPF-certificaat mislukken.

> **Waarschuwing**: als u het CAPF-certificaat regenereert of een door derden ondertekend CAPF-certificaat importeert terwijl de CAPF-service is geactiveerd en gestart, worden telefoons automatisch gereset door CUCM. Voltooi deze procedures in een onderhoudsvenster wanneer het voor telefoons om aanvaardbaar is worden teruggesteld. Zie Cisco bug-id, CSCue55353 - Waarschuwing toevoegen bij herstellen van certificaat TVS/CCM/CAPF dat terugstelt via telefoons

---

> **Opmerking**: als uw CUCM-versie SBD ondersteunt, is deze LSC installatieprocedure van toepassing ongeacht of uw CUCM-cluster is ingesteld op gemengde modus of niet. SBD maakt deel uit van CUCM versie 8.0(1) en hoger. In deze versies van CUCM, de ITL-bestanden bevat het certificaat voor de CAPF-service op de CUCM Publisher. Hierdoor kunnen telefoons verbinding maken met de CAPF-service om certificaatbewerkingen zoals installatie/upgrade en probleemoplossing te ondersteunen.

> In de vorige versies van CUCM, was het noodzakelijk om de cluster voor Gemengde modus te configureren om certificaatbewerkingen te ondersteunen. Aangezien dit niet langer nodig is, vermindert dit barrières voor het gebruik van LSCs als telefoon identiteitscertificaten voor 802.1X-verificatie of voor AnyConnect VPN-clientverificatie.

Draai de opdracht **show itl** op alle TFTP-servers in het CUCM-cluster. Merk op dat het ITL-bestand geen CAPF-certificaat bevat.

Hier is bijvoorbeeld een fragment van de output van de **show** uit de lab CUCM Subscriber ao115sub.

> **Opmerking**: dit bestand bevat een ITL Record-vermelding met een FUNCTIE van CAPF.

> **Opmerking**: Als uw ITL-bestand geen CAPF-vermelding heeft, logt u in bij uw CUCM-uitgever en bevestigt u dat de CAPF-service is geactiveerd. Om dit te bevestigen, navigeer dan naar **Cisco Unified Servicability > Tools > Service Activering > CUCM Publisher > Security**, en activeer vervolgens de **Cisco Certificate Authority Proxy Functie Service**. Als de service is gedeactiveerd en u deze zojuist hebt geactiveerd, navigeer dan naar **Cisco Unified Servicability > Tools > Control Center - Feature Services > Server > CM Services**, start vervolgens de Cisco TFTP-service opnieuw op alle TFTP-servers in het CUCM-cluster om het ITL-bestand te regenereren. Zorg er ook voor dat u niet op Cisco-bug-id CSCuj7830 drukt.

> **Opmerking**: Nadat u klaar bent, voert u de opdracht **show itl** op alle TFTP-servers in het CUCM-cluster uit om te verifiëren dat het huidige CUCM Publisher CAPF-certificaat nu in het bestand is opgenomen.

<#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

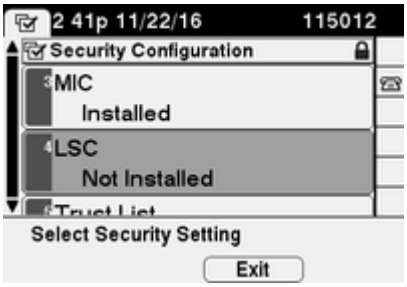
BYTEPOS TAG LENGTH VALUE

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

Als de CAPF-vermelding in het ITL wordt bevestigd, kunt u een certificaatbewerking op een telefoon uitvoeren. In dit voorbeeld, wordt een 2048 bit RSA certificaat geïnstalleerd door gebruik van Null String verificatie.

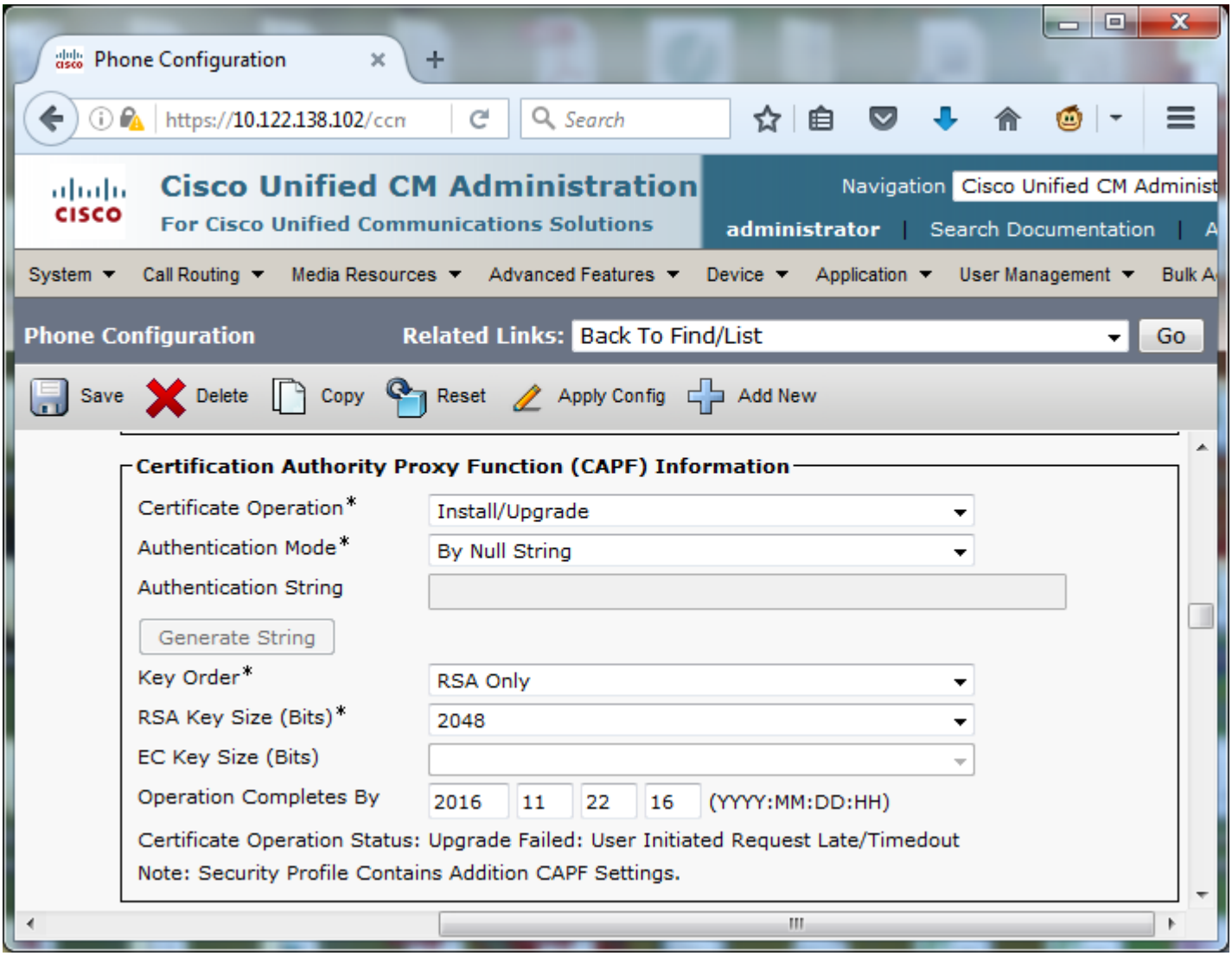
Controleer op de telefoon of een LSC nog niet geïnstalleerd is zoals in de afbeelding. Ga bijvoorbeeld op een telefoon uit de 79XX-serie naar **Instellingen > 4 - Beveiligingsconfiguratie > 4 - LSC**.



Open de telefoon configuratie pagina voor uw telefoon. Navigeer naar **Cisco Unified CM-beheer > Apparaat > Telefoon**.

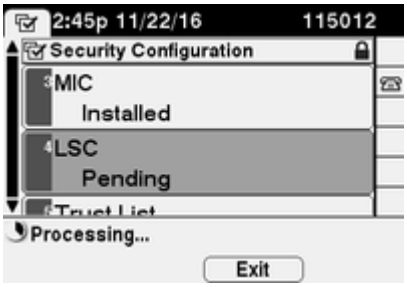
Voer deze gegevens in bij de sectie CAPF-informatie van de configuratie van de telefoon, zoals in de afbeelding:

- Kies **Installeren/upgraden** voor **de** werking van het certificaat
- Voor de Wijze van de Verificatie, kies **door Ongeldige Koord**
- Laat bij dit voorbeeld de sleutelvolgorde, RSA sleutelgrootte (bits) en EC sleutelgrootte (bits) ingesteld op de standaardinstellingen van het systeem.
- Voor Verrichting Voltooit langs, ga een datum en een tijd in die minstens één uur in de toekomst zijn.

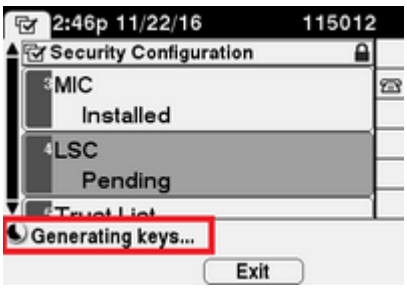


Sla uw configuratiewijzigingen op en **pas** vervolgens **Config toe**.

De status LSC op de telefoon verandert in Pending zoals getoond in het beeld.



De telefoon genereert toetsen zoals in de afbeelding.



De telefoon stelt, en wanneer het terugstellen voltooit, de telefoon LSC status verandert in Geïnstalleerd zoals getoond in het beeld.

Dit is ook zichtbaar onder Status Berichten in de telefoon zoals getoond in de afbeelding.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Raadpleeg het gedeelte Generate CAPF Report van de Security Guide voor Cisco Unified Communications Manager, release 11.0(1) om de installatie van LSC-certificaten op meerdere telefoons te controleren. U kunt ook dezelfde gegevens bekijken in de CUCM-webinterface voor beheer door gebruik te maken van de procedure voor de LSC-status of het verificatietekenreeks.

Raadpleeg het gedeelte Hoe u certificaten kunt ophalen van Cisco IP-telefoon om kopieën te verkrijgen van de LSC-certificaten die in telefoons zijn geïnstalleerd.

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

Geen geldige CAPF-server

De LSC kan niet worden geïnstalleerd. De Berichten van de Status van de telefoon tonen **Geen geldige CAPF server**. Dit geeft aan dat er geen CAPF-ingang in het ITL-bestand is. Controleer dat de CAPF-service is geactiveerd en start vervolgens de TFTP-service opnieuw. Controleer dat het ITL-bestand een CAPF-certificaat bevat na het opnieuw opstarten, stel de telefoon opnieuw in om het laatste ITL-bestand op te nemen en probeer vervolgens uw certificaathandeling opnieuw. Als de CAPF-serververmelding in het menu met beveiligingsinstellingen van de telefoon als hostnaam of volledig gekwalificeerde domeinnaam wordt weergegeven, bevestig dan dat de telefoon in staat is om de vermelding naar een IP-adres op te lossen.

LSC: verbinding mislukt

De LSC kan niet worden geïnstalleerd. De de statusberichten van de telefoon tonen **LSC: De verbinding ontbrak**. Dit kan wijzen op een van deze aandoeningen:

- Als het CAPF-certificaat in het ITL-bestand niet overeenkomt met het huidige certificaat, wordt de CAPF-service gebruikt.
- De CAPF-service wordt gestopt of gedeactiveerd.
- De telefoon kan de CAPF service niet bereiken via het netwerk.

Controleer of de CAPF-service is geactiveerd, start de CAPF-service opnieuw op, start de TFTP-services clusterbreed opnieuw, stel de telefoon opnieuw in om het laatste ITL-bestand op te nemen en probeer vervolgens uw certificaathandeling opnieuw. Als het probleem blijft bestaan, neemt u een pakketopname van de telefoon en de CUCM-uitgever en analyseert u deze om te zien of er sprake is van bidirectionele communicatie op poort 3804, de standaard CAPF-servicepoort. Als dit niet het geval is, kan er een netwerkprobleem zijn.

LSC: mislukt

De LSC kan niet worden geïnstalleerd. De de statusberichten van de telefoon tonen **LSC: Ontbroken**. De webpagina voor telefoonconfiguratie toont de **status van de certificaatbewerking: upgrade mislukt: door gebruiker geïnitieerde aanvraag laat/time-out**. Dit geeft aan dat de bewerking op tijd en datum is voltooid of in het verleden is verlopen. Voer een datum en tijd in die minimaal een uur in voor de toekomst en probeer vervolgens de certificaatbewerking opnieuw.

LSC: Handeling in behandeling

De LSC kan niet worden geïnstalleerd. De statusberichten van de telefoon tonen **LSC: verbinding mislukt**. De pagina van de telefoon Configuratie toont **CertificaatVerrichtingsstatus: Hangende Verrichting.** Er zijn verschillende redenen dat je de **status** van **Certificaat Operatie** kunt zien**: de** status **Operatie in behandeling**. Enkele van hen kunnen omvatten:

- ITL op de telefoon is anders dan die momenteel wordt gebruikt op de samengestelde TFTP-servers.
- Problemen met corrupte ITL's. Wanneer dit gebeurt, verliezen apparaten hun vertrouwde status en de commando **hulpprogramma's zijn gereset localkey** moet worden uitgevoerd van de CUCM Publisher om de telefoons te dwingen om nu het ITLRrecovery certificaat te gebruiken. Als het cluster in de gemengde modus staat, moet u de commando **hulpprogramma's ctl reset localkey** gebruiken**.** Daarna, ziet u een voorbeeld van wat u kunt zien wanneer u probeert om een corrupte ITL van de CLI van CUCM te bekijken. Als er een fout is wanneer u probeert om het ITL te bekijken en probeert om de **hulpprogramma's** in werking te stellen **itl reset localkey** opdracht, maar u ziet de tweede fout, kan dit een defect Cisco bug ID CSCus3755. Bevestig als de versie van de CUCM wordt beïnvloed.

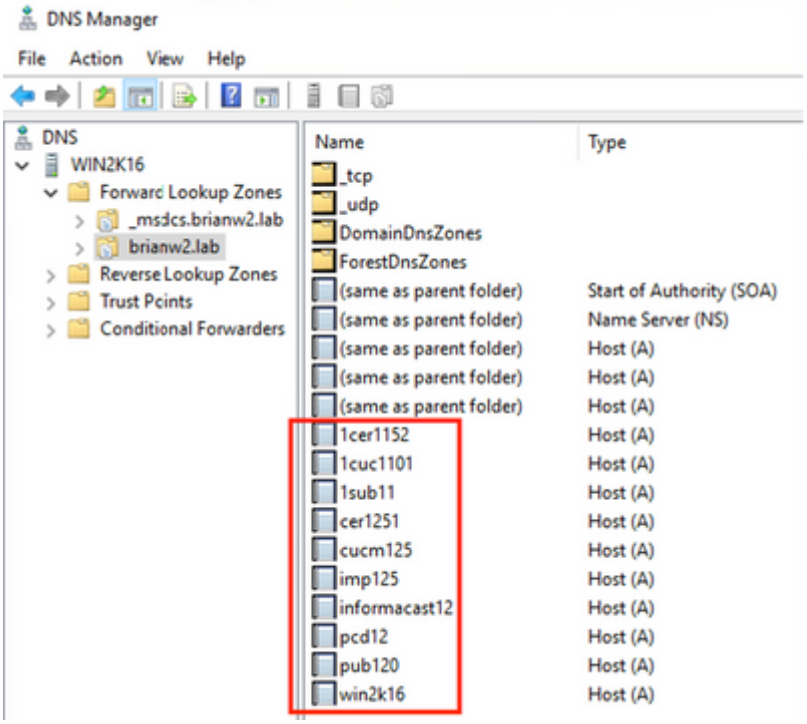
```
admin:show itl
Length of ITL file: 0
ITL File not found. To generate an ITL file, activate or restart the Cisco TFTP service as thi
servers.
Error parsing the ITL File.


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 en
Then retry the command

Executed command unsuccessfully
chmod: changing permissions of `/var/log/active/cm/trace/dbl/sdi/replication_scripts_output
```

- Telefoons kunnen de nieuwe LSC niet verifiëren vanwege een TVS-storing.
- Telefonisch gebruik maken van het MIC certificaat, maar in het gedeelte met de informatie over de certificaatautoriteit (CAPF) op de configuratiepagina van de telefoon is de verificatiemodus ingesteld op door bestaand certificaat (voorrang voor LSC).
- De telefoon kan de FQDN van CUCM niet oplossen.

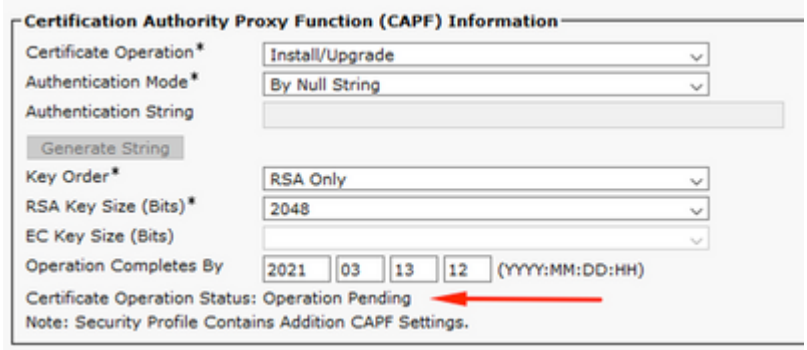
Voor het laatste scenario, is een laboratoriummilieu opstelling om te simuleren wat u in de logboeken zou zien als een telefoon niet FQDN van CUCM kon oplossen. Momenteel, is het laboratorium opstelling met deze servers:

- CUCM Publisher en Subscriber met versie 11.5.1.15038-2
- Windows 2016 Server instellen als mijn DNS-server

Voor de test is er geen DNS-vermelding voor de PUB11 CUCM-server geconfigureerd.



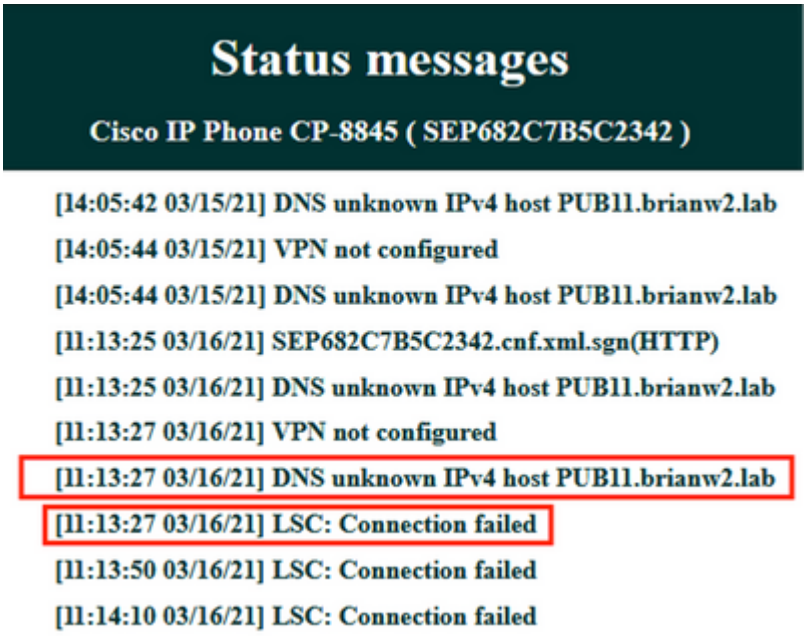
Poging om een LSC naar een van de telefoons (8845) in het lab te duwen. Zie dat het nog steeds Certificaat Handeling Status: Handeling in behandeling toont.



In de logboeken van de telefoonconsole, zie de telefoonpogingen om zijn lokaal geheim voorgeheugen (127.0.0.1) te vragen, voorafgaand aan voorwaartse de vraag aan het gevormde DNS serveradres.

```
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:? - DNS

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

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 for

0632 NOT Mar 12 15:07:55.760715 (12905:13036) JAVA-configmgr MQThread|cip.sec.CertificateProperty:? - Ce
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 addre

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 Tv
```

Zie in de telefoon status berichten hieronder, dat de telefoon niet in staat is om PUB11.brianw2.lab op te lossen. Zie vervolgens het bericht **LSC: Connection is mislukt**.



Te overwegen defecten:

Cisco bug-id CSCub6243 - LSC installatie mislukt met tussenpozen en daarna bevriest het de CAPF Server

Te overwegen defect voor verbetering:

Cisco bug-id CSCuz18034 - rapportage nodig voor geïnstalleerde LSC-endpoints, samen met de vervalstatus

Gerelateerde informatie

Deze documenten bieden meer informatie over het gebruik van LSCâ€™s in de context voor AnyConnect VPN-clientverificatie en 802.1X-verificatie.

- AnyConnect VPN-telefoon - IP-telefoons, ASA en CUCM-probleemoplossing
- Op identiteit gebaseerde netwerkservices: IP-telefonie in IEEE 802.1X-Enabled Networks implementation and Configuration Guide

Er is ook een geavanceerd type LSC-configuratie, waarin de LSC-certificaten rechtstreeks worden ondertekend door een derde partij Certificaatautoriteit, niet het CAPF-certificaat.

Raadpleeg voor meer informatie: CUCM Third-Party CA-Signed LSCs Generation and Import Configuration Voorbeeld

- Technische ondersteuning en documentatie â€“ Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.