

Konfigurieren von LSC auf IP-Telefonen mit CUCM

Inhalt

- [Einleitung](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Hintergrundinformationen](#)
- [MICs und LSCs](#)
- [Konfigurieren](#)
- [Netzwerktopologie](#)
- [Überprüfung](#)
- [Fehlerbehebung](#)
- [Kein gültiger CAPF-Server](#)
- [LSC: Verbindung fehlgeschlagen](#)
- [LSC: Fehler](#)
- [LSC: Vorgang ausstehend](#)
- [Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Installation eines LSC (Locally Significant Certificate) auf einem Cisco IP-Telefon (Cisco IP Phone) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Unified Communications Manager (CUCM) Cluster Security Mode-Optionen
- X.509-Zertifikate
- MICs (Manufacturing Installed Certificates)
- LSCs
- CAPF-Zertifikatvorgänge (Certificate Authority Proxy Function)
- Standardmäßige Sicherheit (Security by Default, SBD)
- ITL-Dateien (Initial Trust List)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf CUCM-Versionen, die SBD unterstützen, d. h. CUCM 8.0(1) und höher.

Hinweis: Dies gilt nur für Telefone, die standardmäßig Security By Default (SBD) unterstützen. Beispielsweise unterstützen die Telefone 7940 und 7960 weder SBD noch die Konferenztelefone 7935, 7936 und 7937. Eine Liste der Geräte, die SBD in Ihrer CUCM-Version unterstützen, finden Sie

unter **Cisco Unified Reporting > System Reports > Unified CM Phone Feature List (Cisco Unified Reporting > Systemberichte > Unified CM Phone-Funktionsliste)**, und führen Sie einen Bericht zu Feature: Security By Default (Funktion: Sicherheit standardmäßig) aus.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

MICs und LSCs

Wenn Sie eine zertifikatbasierte Authentifizierung für 802.1X oder AnyConnect Phone VPN verwenden, ist es wichtig, den Unterschied zwischen MICs und LSCs zu verstehen.

Jedes Cisco Telefon wird mit einem werkseitig vorinstallierten MIC geliefert. Dieses Zertifikat wird von einem der Zertifikate der Cisco Manufacturing CA signiert, entweder vom Cisco Manufacturing CA-, Cisco Manufacturing CA SHA2-, CAP-RTP-001- oder CAP-RTP-002-Zertifikat. Wenn das Telefon dieses Zertifikat präsentiert, weist es nach, dass es sich um ein gültiges Cisco Telefon handelt. Dies bestätigt jedoch nicht, dass das Telefon zu einem bestimmten Kunden oder CUCM-Cluster gehört. Es könnte sich dabei um ein unautorisiertes Telefon handeln, das auf dem freien Markt erworben oder von einem anderen Standort aus genutzt wird.

LSCs dagegen werden von einem Administrator absichtlich auf Telefonen installiert und vom CAPF-Zertifikat des CUCM Publisher signiert. Sie sollten 802.1X oder AnyConnect VPN so konfigurieren, dass nur LSCs vertrauenswürdig sind, die von bekannten CAPF-Zertifizierungsstellen ausgestellt wurden. Wenn Sie die Zertifikatsauthentifizierung auf LSCs anstatt auf MICs basieren, erhalten Sie eine viel detailliertere Kontrolle darüber, welchen Telefongeräten vertraut wird.

Konfigurieren

Netzwerktopologie

Die folgenden CUCM-Lab-Server wurden für dieses Dokument verwendet:

- ao115pub - 10.12.138.102 - CUCM Publisher und TFTP-Server
- ao115sub - 10.122.138.103 - CUCM-Subscriber und TFTP-Server

Vergewissern Sie sich, dass das CAPF-Zertifikat noch nicht abgelaufen ist und in naher Zukunft ablaufen wird. Navigieren Sie zu **Cisco Unified OS Administration > Security > Certificate Management**, und **suchen Sie dann nach der Zertifikatsliste, in der das Zertifikat genau den CAPF-Wert hat**, wie im Bild dargestellt.

The screenshot displays the Cisco Unified Operating System Administration interface for managing certificates. The page title is "Certificate List" and the URL is "https://10.122.138.102/cmplatform/certificateFindList.do". The user is logged in as "administrator".

Navigation options include: Show, Settings, Security, Software Upgrades, Services, Help.

Actions available: Generate Self-signed, Upload Certificate/Certificate chain, Generate CSR.

Status: 1 records found

Filter: Find Certificate List where Certificate is exactly CAPF

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	
CAPF	CAPF-7f0ae8d7	Self-signed	RSA	ao115pub	CAPF-7f0ae8d7	11/20/2021	Self-sign

Actions available below the table: Generate Self-signed, Upload Certificate/Certificate chain, Generate CSR.

Klicken Sie auf **Gemeinsamer Name**, um die Seite Zertifikatdetails zu öffnen. Überprüfen Sie das Datum Gültig von: und das Datum Bis: im Bereich **Zertifikatsdateidaten**, um zu bestimmen, wann das Zertifikat abläuft, wie im Bild gezeigt.

Certificate Details(Self-signed) - Mozilla Firefox

https://10.122.138.102/cmplatform/certificateEdit.do?cert=/usr/local/cm/.security/CAPF/certs/CAPF.pem/CAPF.

Certificate Details for CAPF-7f0ae8d7, CAPF

Regenerate Generate CSR Download .PEM File Download .DER File

Status

Status: Ready

Certificate Settings

File Name	CAPF.pem
Certificate Purpose	CAPF
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Self-signed certificate generated by system

Certificate File Data

```
[
Version: V3
Serial Number: 64F2FE613B79C5D362E26DAB4A8B761B
Signature Algorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: L=Boxborough, ST=MA, CN=CAPF-7f0ae8d7, OU=TAC, O=Cisco Systems, C=US
Validity From: Mon Nov 21 15:49:43 EST 2016
To: Sat Nov 20 15:49:42 EST 2021
Subject Name: L=Boxborough, ST=MA, CN=CAPF-7f0ae8d7, OU=TAC, O=Cisco Systems, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100c39c51d51eadb8216af79a1b231ce42896cf13fd23293f32a2f0baea679e5fa1ac5
bb58fcf015c179272e4f470ec06900667997de25c7bc61653d4302c8adc4022bb2bee47f9a7b56adfd5c5
4770f41f06bf5e4621e2a8233146a7fccd40d55704cd73a03a44f5b674cbec81e33c06d5d44e358db4b8
9710b4c022bc4357a1a064df9e8e02e9feb00213f0c0bd8bde9a363d6afcf162c20a86561d3e87acad8b
02cf079b01cfa3afdd12197bc115cb478202d41b5389dc0b8676c61011d73eb3f1e2bf3f204a4da2f753a
c2d88b1a5ab759abdb4453eda89713592dde471c23884dc738c7ed2f1c6d0b393678cec88d1bad2746d
```

Regenerate Generate CSR Download .PEM File Download .DER File

Close

Wenn das CAPF-Zertifikat abgelaufen ist oder bald ablaufen wird, generieren Sie das Zertifikat neu. Fahren Sie nicht mit dem LSC-Installationsprozess mit einem abgelaufenen oder bald ablaufenden CAPF-Zertifikat fort. Auf diese Weise wird vermieden, dass LSCs nach Ablauf des CAPF-Zertifikats in naher Zukunft neu ausgestellt werden müssen. Weitere Informationen zum Neugenerieren des CAPF-Zertifikats finden Sie im Artikel [zum Neugenerieren/Erneuern von CUCM-Zertifikaten](#).

Ebenso haben Sie in dieser Phase die Möglichkeit, Ihr CAPF-Zertifikat von einer unabhängigen Zertifizierungsstelle signieren zu lassen. Führen Sie jetzt entweder die Erstellung der CSR-Datei (Certificate Signing Request) und den Import des signierten CAPF-Zertifikats aus, oder setzen Sie die Konfiguration mit einem selbstsignierten LSC für einen ersten Test fort. Wenn Sie ein von einem Drittanbieter signiertes CAPF-Zertifikat benötigen, ist es in der Regel sinnvoll, diese Funktion zuerst mit einem selbstsignierten

CAPF-Zertifikat zu konfigurieren, LSCs zu testen und zu überprüfen und dann erneut bereitzustellen, die von einem von einem Drittanbieter signierten CAPF-Zertifikat signiert werden. Dies vereinfacht die spätere Fehlerbehebung, wenn die Tests mit dem von einem Drittanbieter signierten CAPF-Zertifikat fehlschlagen.

Warnung: Wenn Sie das CAPF-Zertifikat neu generieren oder ein von einem Drittanbieter signiertes CAPF-Zertifikat importieren, während der CAPF-Dienst aktiviert und gestartet wird, werden die Telefone automatisch vom CUCM zurückgesetzt. Führen Sie diese Schritte in einem Wartungsfenster aus, wenn Telefone zurückgesetzt werden können. Weitere Informationen finden Sie unter Cisco Bug-ID [CSCue55353 - Hinzufügen einer Warnung beim Regenerieren des TVS/CCM/CAPF-Zertifikats, das von Telefonen zurückgesetzt wird.](#)

Hinweis: Wenn Ihre CUCM-Version SBD unterstützt, gilt dieses LSC-Installationsverfahren unabhängig davon, ob Ihr CUCM-Cluster auf den gemischten Modus eingestellt ist. SBD ist Teil von CUCM Version 8.0(1) und höher. In diesen Versionen von CUCM enthalten die ITL-Dateien das Zertifikat für den CAPF-Dienst auf dem CUCM Publisher. Dadurch können sich Telefone mit dem CAPF-Dienst verbinden, um Zertifikatvorgänge wie Installation/Upgrade und Fehlerbehebung zu unterstützen.

In den früheren Versionen von CUCM war es erforderlich, den Cluster für den gemischten Modus zu konfigurieren, um Zertifikatvorgänge zu unterstützen. Da dies nicht mehr erforderlich ist, werden die Hindernisse für die Verwendung von LSCs als Telefon-Identitätszertifikate für die 802.1X-Authentifizierung oder die AnyConnect VPN-Client-Authentifizierung beseitigt.

Führen Sie den Befehl **show itl** auf allen TFTP-Servern im CUCM-Cluster aus. Beachten Sie, dass die ITL-Datei ein CAPF-Zertifikat enthält.

Dies ist beispielsweise ein Auszug aus der **show itl**-Ausgabe des CUCM-Subscribers ao115sub.

Hinweis: Diese Datei enthält einen ITL-Eintrag mit der FUNKTION CAPF.

Hinweis: Wenn Ihre ITL-Datei keinen CAPF-Eintrag enthält, melden Sie sich bei Ihrem CUCM-Publisher an, und bestätigen Sie, dass der CAPF-Service aktiviert ist. Um dies zu bestätigen, navigieren Sie zu **Cisco Unified Serviceability > Tools > Service Activation > CUCM Publisher > Security**, und aktivieren Sie dann den **Cisco Certificate Authority Proxy Function Service**. Wenn der Service deaktiviert und gerade aktiviert wurde, navigieren Sie zu **Cisco Unified Serviceability > Tools > Control Center - Feature Services > Server > CM Services**, und starten Sie den Cisco TFTP-Service auf allen TFTP-Servern im CUCM-Cluster neu, um die ITL-Datei neu zu generieren. Achten Sie außerdem darauf, dass Sie die Cisco Bug-ID [CSCuj78330](#) nicht erreichen.

Hinweis: Führen Sie nach Abschluss des Vorgangs den Befehl **show itl** auf allen TFTP-Servern im CUCM-Cluster aus, um zu überprüfen, ob das aktuelle CAPF-Zertifikat des CUCM Publisher jetzt in der Datei enthalten ist.

<#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

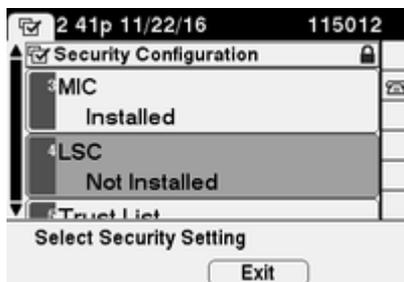
1 RECORDLENGTH 2 1031
2 DNSNAME 9 ao115sub

```
3 SUBJECTNAME 62 CN=ao115sub-EC;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TFTP
5 ISSUERNAM 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.

Nachdem der CAPF-Eintrag als Eintrag im ITL bestätigt wurde, können Sie einen Zertifikatvorgang auf einem Telefon abschließen. In diesem Beispiel wird ein 2048-Bit-RSA-Zertifikat mithilfe der Null-String-Authentifizierung installiert.

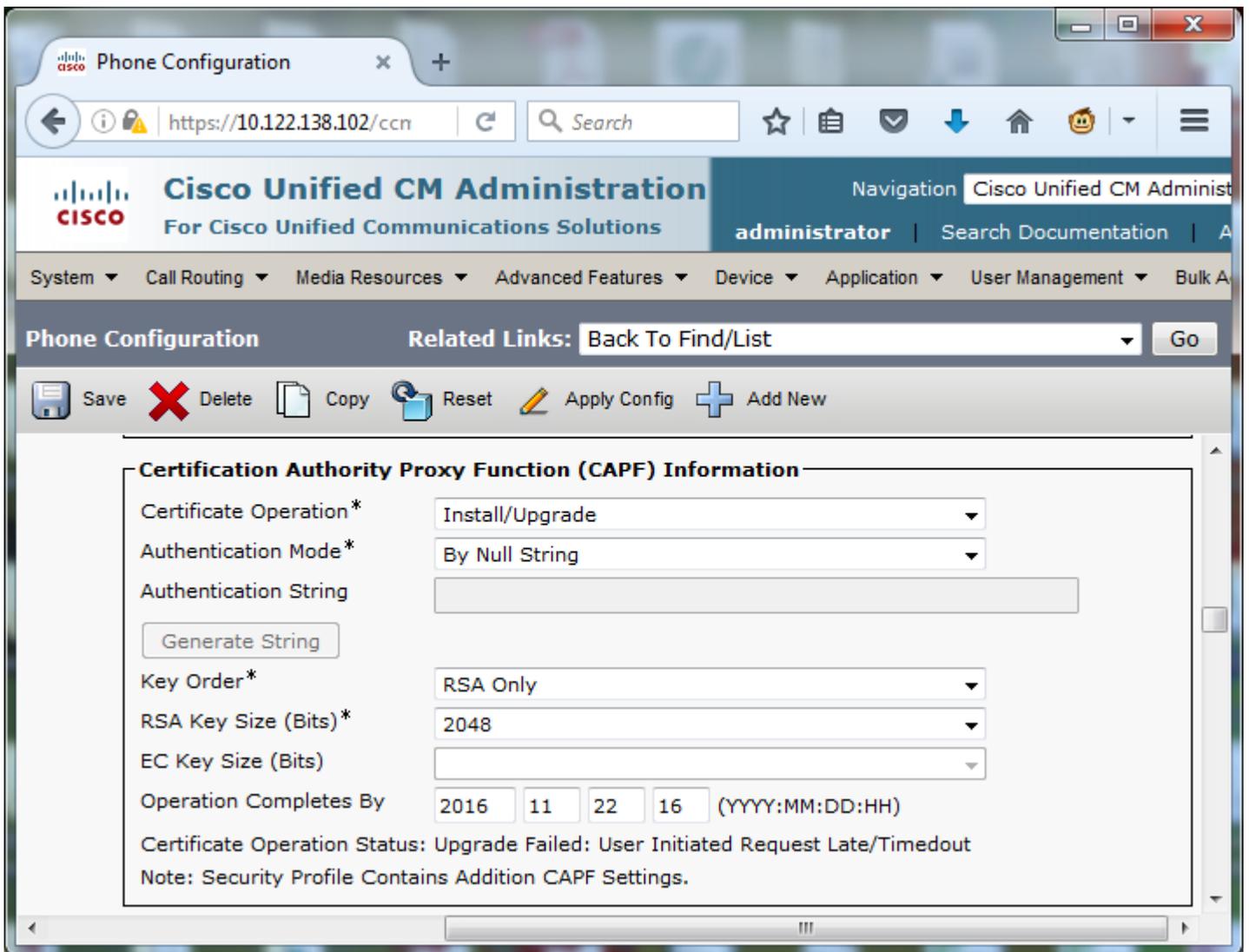
Überprüfen Sie am Telefon, ob noch kein LSC installiert ist, wie im Bild gezeigt. Navigieren Sie z. B. auf einem Telefon der Serie 79XX zu **Einstellungen > 4 - Sicherheitskonfiguration > 4 - LSC**.



Öffnen Sie die Seite für die Telefonkonfiguration Ihres Telefons. Navigieren Sie zu **Cisco Unified CM Administration > Device > Phone (Gerät > Telefon)**.

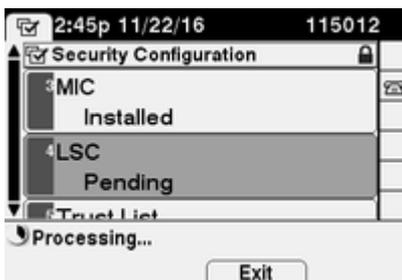
Geben Sie im Bereich "CAPF Information" (CAPF-Informationen) der Konfiguration des Telefons die folgenden Details ein, wie im Bild gezeigt:

- Wählen Sie für den Zertifikatvorgang **Install/Upgrade (Installieren/Aktualisieren)**.
- Wählen Sie für den Authentifizierungsmodus **By Null String (Nach NULL-Zeichenfolge) aus**.
- Lassen Sie für dieses Beispiel die Schlüsselreihenfolge, die RSA-Schlüsselgröße (Bits) und die EC-Schlüsselgröße (Bits) auf die Systemstandardwerte festgelegt.
- Geben Sie für "Arbeitsvorgang abgeschlossen bis" ein Datum und eine Uhrzeit ein, die mindestens eine Stunde in der Zukunft liegen.

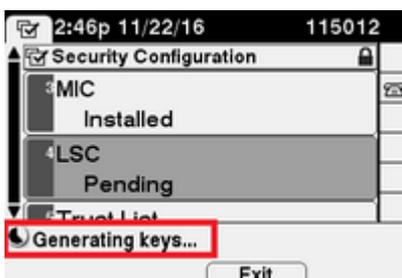


Speichern Sie die Konfigurationsänderungen, und wenden Sie die Konfiguration an.

Der LSC-Status auf dem Telefon ändert sich in Ausstehend, wie im Bild gezeigt.



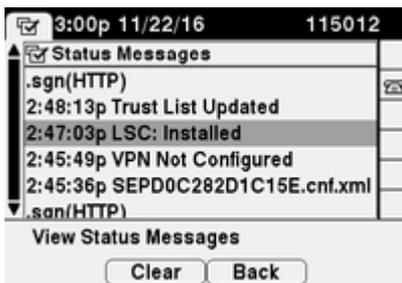
Das Telefon generiert Schlüssel, wie im Bild dargestellt.



Das Telefon wird zurückgesetzt, und wenn das Zurücksetzen abgeschlossen ist, ändert sich der LSC-Status des Telefons in Installed (Installiert), wie im Bild gezeigt.



Dies wird auch unter "Statusmeldungen" im Telefon angezeigt, wie im Bild gezeigt.



Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Informationen zur Überprüfung der Installation von LSC-Zertifikaten auf mehreren Telefonen finden Sie im Abschnitt [Generate CAPF Report \(CAPF-Bericht generieren\)](#) im [Security Guide for Cisco Unified Communications Manager, Release 11.0\(1\)](#). Alternativ können Sie die gleichen Daten auch in der CUCM-Administration-Webschnittstelle anzeigen, indem Sie die Prozedur "[Telefone nach LSC-Status suchen](#)" oder "[Authentifizierungszeichenfolge verwenden](#)".

Informationen zum Abrufen von Kopien der in Telefonen installierten LSC-Zertifikate finden Sie im Artikel [Abrufen von Zertifikaten von Cisco IP-Telefonen](#).

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Kein gültiger CAPF-Server

Das LSC kann nicht installiert werden. Die Statusmeldungen des Telefons zeigen **keinen gültigen CAPF-Server an**. Dies weist darauf hin, dass in der ITL-Datei kein CAPF-Eintrag vorhanden ist. Überprüfen Sie, ob der CAPF-Dienst aktiviert wurde, und starten Sie dann den TFTP-Dienst neu. Überprüfen Sie nach dem Neustart, ob die ITL-Datei ein CAPF-Zertifikat enthält, setzen Sie das Telefon zurück, um die neueste ITL-Datei abzurufen, und wiederholen Sie dann den Zertifikatvorgang. Wenn der CAPF-Servereintrag im Menü mit den Sicherheitseinstellungen des Telefons als Hostname oder vollständig qualifizierter Domänenname angezeigt wird, stellen Sie sicher, dass das Telefon den Eintrag in eine IP-Adresse auflösen kann.

LSC: Verbindung fehlgeschlagen

Das LSC kann nicht installiert werden. Die Statusmeldungen des Telefons zeigen **LSC: Connection Failed (LSC: Verbindung fehlgeschlagen)**. Dies kann auf eine der folgenden Bedingungen hinweisen:

- Wenn das CAPF-Zertifikat in der ITL-Datei nicht mit dem aktuellen Zertifikat übereinstimmt, wird der CAPF-Dienst verwendet.
- Der CAPF-Dienst wird beendet oder deaktiviert.
- Das Telefon kann den CAPF-Dienst nicht über das Netzwerk erreichen.

Überprüfen Sie, ob der CAPF-Dienst aktiviert ist, starten Sie den CAPF-Dienst neu, starten Sie die TFTP-Dienste clusterweit neu, setzen Sie das Telefon zurück, um die neueste ITL-Datei abzurufen, und wiederholen Sie dann den Zertifikatvorgang. Wenn das Problem weiterhin besteht, erfassen Sie die Pakete vom Telefon und vom CUCM Publisher, und analysieren Sie, um festzustellen, ob auf Port 3804, dem standardmäßigen CAPF-Service-Port, eine bidirektionale Kommunikation besteht. Andernfalls kann es zu einem Netzwerkproblem kommen.

LSC: Fehler

Das LSC kann nicht installiert werden. Die Statusmeldungen des Telefons zeigen **LSC an: Failed (Fehlgeschlagen)**. Auf der Webseite für die Telefonkonfiguration wird der **Status des Zertifikatvorgangs** angezeigt: **Upgrade Failed: User Initiated Request Late/Timeout (Upgrade fehlgeschlagen) (Vom Benutzer initiierte Anforderung verspätet/Timeout)**. Dies zeigt an, dass der Vorgang "Abgeschlossen nach" abgelaufen ist oder in der Vergangenheit liegt. Geben Sie ein Datum und eine Uhrzeit ein, die mindestens eine Stunde in der Zukunft liegen, und wiederholen Sie dann den Zertifikatvorgang.

LSC: Vorgang ausstehend

Das LSC kann nicht installiert werden. Die Statusmeldungen des Telefons zeigen **LSC an: Verbindung fehlgeschlagen**. Auf der Seite für die Telefonkonfiguration wird der **Status des Zertifikatvorgangs** angezeigt: **Vorgang ausstehend**. Es gibt verschiedene Gründe, warum der **Status des Zertifikatvorgangs** angezeigt wird: **Vorgang steht aus**. Dazu gehören u. a.:

- Die ITL auf dem Telefon unterscheidet sich von der derzeit auf den konfigurierten TFTP-Servern verwendeten ITL.
- Probleme mit beschädigten ITLs. In diesem Fall verlieren Geräte ihren vertrauenswürdigen Status, und der Befehl **utils itl reset localkey** muss vom CUCM Publisher ausgeführt werden, damit die Telefone das ITLRecovery-Zertifikat verwenden. Wenn sich der Cluster im gemischten Modus befindet, müssen Sie den Befehl **utils ctl reset localkey** verwenden. Als Nächstes sehen Sie ein Beispiel für die Anzeige einer beschädigten ITL über die CLI von CUCM. Wenn beim Versuch, die ITL anzuzeigen, ein Fehler auftritt und versucht wird, den Befehl **utils itl reset localkey** auszuführen, aber der zweite Fehler angezeigt wird, kann dies ein Fehler mit der Cisco Bug-ID [CSCus33755](#) sein. Bestätigen Sie, ob die Version von CUCM betroffen ist.

```
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
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

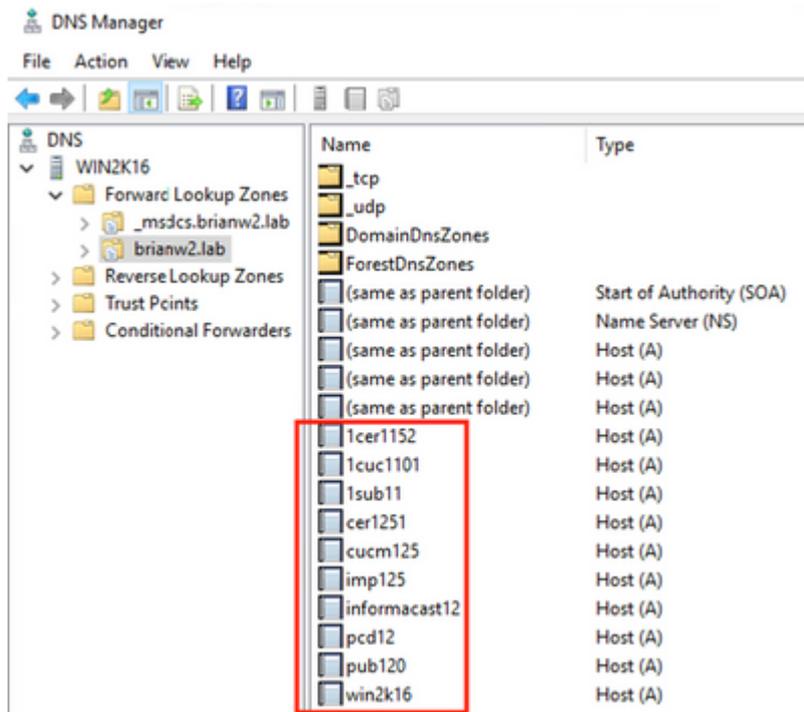
```
Executed command unsuccessfully
chmod: changing permissions of `/var/log/active/cm/trace/dbl/sdi/replication_scripts_output
```

- Telefone können das neue LSC aufgrund eines TVS-Fehlers nicht authentifizieren.
- Das Telefon verwendet das MIC-Zertifikat, aber im Abschnitt CAPF-Informationen (Certificate Authority Proxy Function) auf der Seite für die Telefonkonfiguration wurde der Authentifizierungsmodus durch vorhandenes Zertifikat festgelegt (Precedence zu LSC).
- Das Telefon kann den FQDN des CUCM nicht auflösen.

Im letzten Szenario wird eine Laborumgebung eingerichtet, um zu simulieren, was in den Protokollen angezeigt wird, wenn ein Telefon den FQDN von CUCM nicht auflösen kann. Derzeit umfasst die Übung folgende Server:

- CUCM Publisher und Subscriber mit Version 11.5.1.15038-2
- Windows 2016 Server-Setup als DNS-Server

Für den Test ist kein DNS-Eintrag für den PUB11 CUCM-Server konfiguriert.



Versucht, ein LSC an eines der Telefone (8845) in der Übung zu verschieben. Überprüfen Sie, ob der Status des Zertifikatvorgangs weiterhin "Vorgang ausstehend" angezeigt wird.

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*

Authentication Mode*

Authentication String

Key Order*

RSA Key Size (Bits)*

EC Key Size (Bits)

Operation Completes By (YYYY:MM:DD:HH)

Certificate Operation Status: Operation Pending 

Note: Security Profile Contains Addition CAPF Settings.

Sehen Sie in den Telefonkonsolenprotokollen nach, wie das Telefon versucht, seinen lokalen Cache (127.0.0.1) abzufragen, bevor die Abfrage an die konfigurierte DNS-Serveradresse weitergeleitet wird.

```
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 address

```
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
```

Sehen Sie in den Telefonstatusmeldungen unten, dass das Telefon nicht in der Lage ist, PUB11.brianw2.lab zu lösen. Lesen Sie anschließend die Meldung **LSC: Connection failed (Verbindung fehlgeschlagen)**.

Status messages

Cisco IP Phone CP-8845 (SEP682C7B5C2342)

```
[14:05:42 03/15/21] DNS unknown IPv4 host PUB11.brianw2.lab
[14:05:44 03/15/21] VPN not configured
[14:05:44 03/15/21] DNS unknown IPv4 host PUB11.brianw2.lab
[11:13:25 03/16/21] SEP682C7B5C2342.cnf.xml.sgn(HTTP)
[11:13:25 03/16/21] DNS unknown IPv4 host PUB11.brianw2.lab
[11:13:27 03/16/21] VPN not configured
[11:13:27 03/16/21] DNS unknown IPv4 host PUB11.brianw2.lab
[11:13:27 03/16/21] LSC: Connection failed
[11:13:50 03/16/21] LSC: Connection failed
[11:14:10 03/16/21] LSC: Connection failed
```

Zu berücksichtigende Mängel:

Cisco Bug-ID [CSCub6243](#) - LSC-Installation schlägt gelegentlich fehl und friert danach den CAPF-Server ein

Zu berücksichtigender Erweiterungsfehler:

Cisco Bug-ID [CSCuz18034](#) - Meldung erforderlich, wenn LSC Endgeräte installiert hat, zusammen mit dem Ablaufstatus

Zugehörige Informationen

Diese Dokumente enthalten weitere Informationen zur Verwendung von LSCs im Kontext für die AnyConnect VPN-Client-Authentifizierung und die 802.1X-Authentifizierung.

- [AnyConnect VPN-Telefon - Fehlerbehebung für IP-Telefone, ASA und CUCM](#)
- [Identitätsbasierte Netzwerkdienste: IP-Telefonie in IEEE 802.1X-fähigen Netzwerken - Bereitstellungs- und Konfigurationsleitfaden](#)

Es gibt auch einen erweiterten LSC-Konfigurationstyp, bei dem die LSC-Zertifikate direkt von einer Zertifizierungsstelle eines Drittanbieters signiert werden, nicht vom CAPF-Zertifikat.

Weitere Informationen finden Sie unter [Konfigurationsbeispiel](#) zum [Generieren und Importieren von LSCs mit CA-Signatur von CUCM-Drittanbietern](#).

- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.