

# CUCM の設定 LSC on Cisco IP Phone

## 目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[MIC vs LSCs](#)

[設定](#)

[ネットワークトポロジ](#)

[確認](#)

[トラブルシューティング](#)

[有効な CAPF サーバ無し](#)

[LSC: 接続に失敗しました。](#)

[LSC: Failed \( 故障 \)](#)

[関連情報](#)

## 概要

この資料に Cisco Internet Protocol ( IP ) インストールする方法を電話 ( Cisco IP Phone ) でローカルで固有の証明書 ( LSC ) を記述されています。

## 前提条件

### 要件

次の項目に関する知識が推奨されます。

- Cisco Unified Communications Manager ( CUCM ) クラスタ セキュリティモード オプション
- X.509 証明書
- 製造インストール済み証明書 ( MIC )
- LSCs
- 認証局 ( CA ) プロキシ 機能 ( CAPF ) 証明書 オペレーション
- デフォルトでセキュリティ ( SBD )
- 最初の信頼リスト ( ITL ) ファイル

### 使用するコンポーネント

この文書に記載されている情報は CUCM バージョンに基づいています SBD を、即ち CUCM 8.0(1) 以上にサポートする。

注: それはまた SBD をサポートする電話にしか関係しません。たとえば、7940 台および 7960 台の電話は SBD をサポートしません、7935 台、7936 台および 7937 台の会議電話は

。 CUCM のバージョンの SBD をサポートするデバイスのリストに関しては、Cisco Unified レポート > システム レポートへのナビゲートは > CM 電話 機能 リストを統一し、機能のレポートを送ります: セキュリティ デフォルトで。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

## 背景説明

### MIC vs LSCs

802.1X が Anyconnect 電話 VPN のために証明書によって基づく認証を使用する場合、MIC と LSCs の違いを理解することは重要です。

ファクトリでプレインストールされる各 Cisco Phone は MIC が付いています。この証明書は CA を、Cisco CA SHA2 製造する、Cisco による CA 証明書を、CAP-RTP-001 または CAP-RTP-002 証明書を製造する製造する Cisco の 1 つによって署名します。電話はこの証明書を示すとき、電話が特定の顧客が CUCM クラスターに属することそれが有効な Cisco Phone であるが、これは検証しませんと証明します。それは可能性としては公開市場で購入されるか、または別のサイトから持って来られた不正な電話である可能性があります。

LSCs は、一方では、管理者によって電話で計画的にインストールされ、CUCM パブリッシャの CAPF 証明書によって署名します。既知 CAPF 証明書権限によって発行された LSCs しか信頼しないために 802.1X が Anyconnect VPN を設定します。MIC の代りの LSCs に証明書認証を基づかせていることは電話デバイスが信頼される大いに粒状制御を与えます。

## 設定

### ネットワーク トポロジ

これらの CUCM ラボ サーバはこの資料のために使用されました:

- ao115pub - 10.122.138.102 - CUCM パブリッシャ及び TFTPサーバ
- ao115sub - 10.122.138.103 - CUCM サブスクライバ及び TFTPサーバ

CAPF 証明書が切れなかった確認して下さい、ことを近い将来に切れることを約あります。

Cisco Unified OS 管理 > Security > Certificate Management にナビゲートし、そして証明書がイメージに示すように丁度 CAPF である証明書 リストを見つけて下さい。

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

Status

1 records found

Certificate List (1 - 1 of 1) Rows per Page 50

Find Certificate List where Certificate is exactly CAPF Find Clear Filter

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
	<a href="#">CAPF-7f0ae8d7</a>	Self-signed	RSA	ao115pub	CAPF-7f0ae8d7	11/20/2021	Self-signed certificate generated by system

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

証明書の詳細 ページを開くために **Common Name** をクリックして下さい。有効性をからの点検して下さい: そしてに: 証明書が切れる時証明書ファイル データ ペインの日付、イメージに示すように判別するため。

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, QU=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, QU=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

CAPF 証明書が切れるか、またはすぐに切れることならその証明書を再生するため。期限切れの LSC インストール プロセスと進みませんでしたり、またはすぐに証明書 CAPF 切らさないで下さい。これは CAPF 認証満了による LSCs を近い将来に再発行する必要性を避けます。CAPF 証明書を再生する方法についての情報に関しては [CUCM 証明書再生/再生過程](#) 記事を参照して下さい。

CAPF 証明書をサードパーティによって認証局 (CA) 署名してもらう必要があれば同様にこの段階で作るべき選択があります。どちらかの完全署名された CAPF 証明書の証明書署名要求 (CSR) ファイル 生成および輸入今、または予備テスト用の自己署名 LSC の設定を続けます。サードパーティによって署名される CAPF 証明書を必要とする場合この機能を自己署名 CAPF 証明書で最初に設定し、サードパーティによって署名される CAPF 証明書によって署名する

LSCs をテストし、確認し、次に転用するために、一般に良識があります。これはサードパーティが付いているテストが CAPF 証明書失敗に署名した場合、より遅いトラブルシューティングを簡素化します。

**警告：** CAPF サービスがアクティブになり、開始する間、CAPF 証明書を再生するか、またはサードパーティ署名された CAPF 証明書をインポートすれば、電話は CUCM によって自動的にリセットされます。電話がリセットされることは受諾可能なとき Maintenance ウィンドウのこれらの手順を完了して下さい。参照に関しては、参照して下さい

[CSCue55353 -その TVS/CCM/CAPF 証明書を再生した場合警告を電話をかけますリセットに追加して下さい。](#)

**注:** CUCM クラスタがミックスモードに設定されるかどうか CUCM バージョン サポート SBD が、この LSC インストール手順それにもかかわらず適用すれば。SBD は CUCM バージョン 8.0(1) および それ以降の部分です。CUCM のこれらのバージョンでは、ITL ファイルは CUCM パブリッシャの CAPF サービスのための証明書が含まれています。これは電話がインストール/アップグレードのような証明書 オペレーションをサポートし、解決するために CAPF サービスに接続するようにします。

CUCM の前のバージョンでは、証明書 オペレーションをサポートするためにミックスモードのためのクラスタを設定することは必要でした。これがもはや必要ではないので、これは 802.1X 認証または AnyConnect VPN クライアント 認証のための電話 ID証明として LSCs の使用に障壁を減らします。

CUCM クラスタの TFTP すべてのサーバの**提示 itl** コマンドを実行して下さい。ITL ファイルが含まれている CAPF 証明書がことを観察して下さい。

たとえば、ラボ CUCM サブスクライバ ao115sub から出力される**提示 itl** の抜粋はここにありません。

**注:** CAPF の機能のこのファイルに ITL レコード 記述項があります。

**注:** ITL ファイルに CAPF エントリがない場合、CUCM パブリッシャへのログインは CAPF サービスを確認するためにアクティブになり。これを、ナビゲート Cisco プロキシ 機能サービスを認証局 (CA) アクティブにするために Cisco Unified サービスability > Tools > Service アクティベーションに確認するため > CUCM パブリッシャ > Security、それから。サービスが無効になり、ちょうどそれをアクティブにしたら、Cisco Unified サービスability > Tools > Control Center へのナビゲート-サービス > サーバ > CM サービスを特色にして下さい、ITL ファイルを再生するために CUCM クラスタの TFTP すべてのサーバの Cisco TFTP サービスを再開して下さい。また [CSCuj78330](#) を見つけないように、して下さい。

**注:** 終了した後、電流 CUCM パブリッシャ CAPF 証明書がファイルに今含まれていることを確認するために CUCM クラスタの TFTP すべてのサーバの**提示 itl** コマンドを実行して下さい。

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 ISSUERNAM 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 ISSUERNAM 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 ISSUERNAM 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 ISSUERNAM 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.

ITL のエントリとして確認されて CAPF エントリが電話の証明書 オペレーションを完了できます。この例では、2048 ビット RSA 証明書はヌルストリング 認証を使用してインストールされています。

電話で、LSC がイメージに示すようにまだインストールされていないことを確認して下さい。たとえば、79XX シリーズ電話で、設定へのナビゲート > 4 -セキュリティとコンフィギュレーション > 4 - LSC。

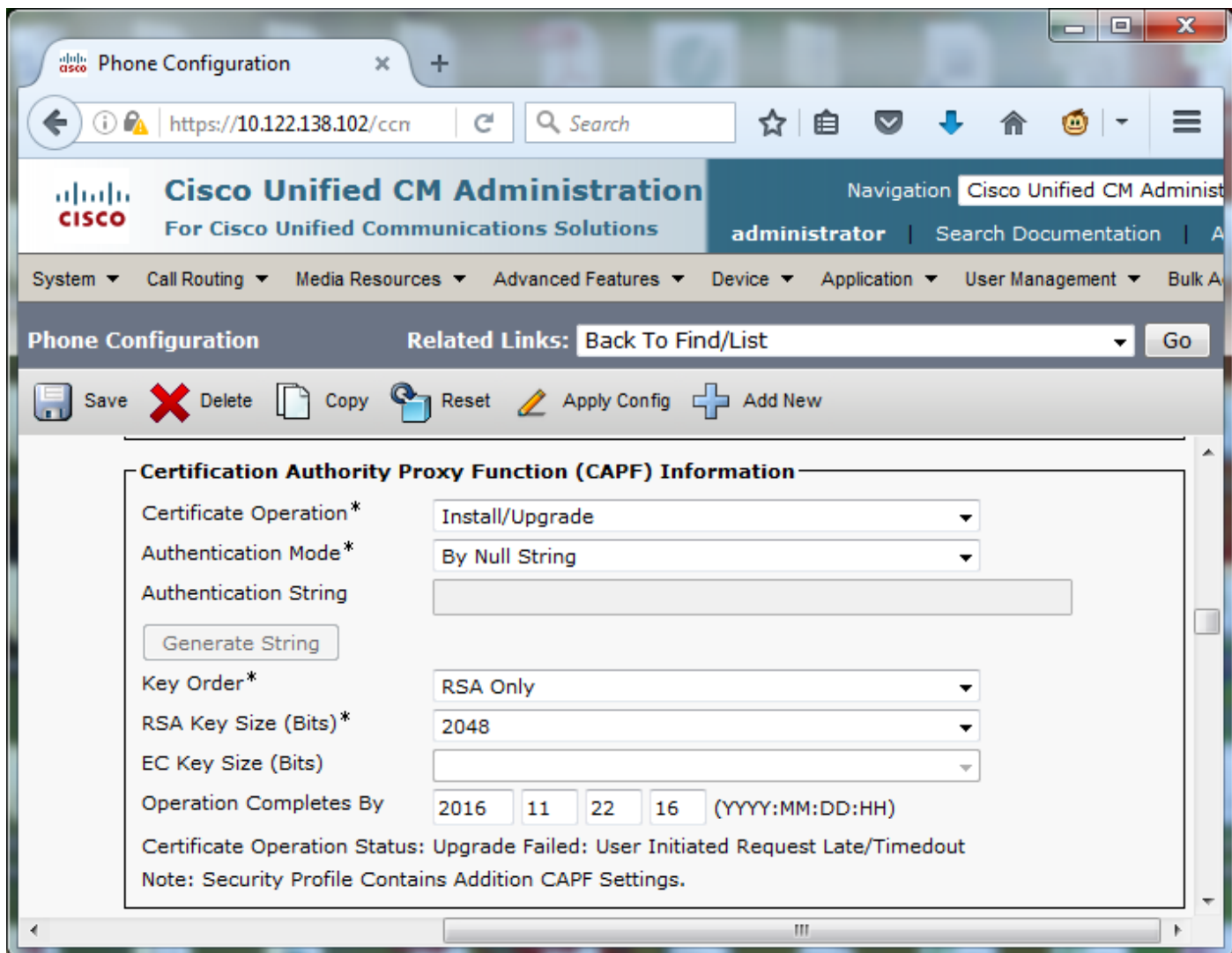


電話のための Phone Configuration ページを開いて下さい。Cisco Unified CM Administration > Device > Phone へのナビゲート。

イメージに示すように電話の設定の CAPF インフォメーション セクションにこれらの詳細を、入力して下さい:

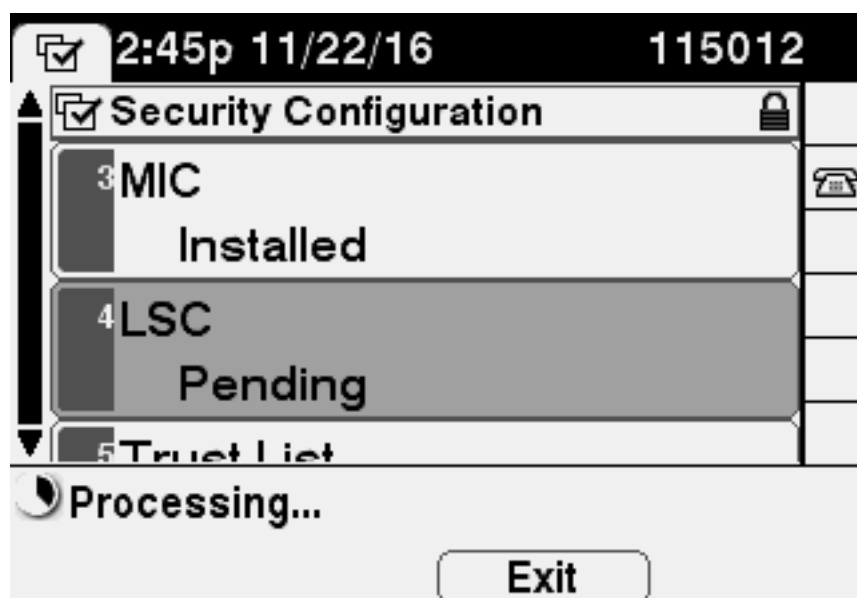
- 証明書 オペレーションに関しては、『Install』を選択して下さい/アップグレード
- 認証モードに関しては、**ヌルストリング**によって選択して下さい
- この例に関しては、キー順序、RSA キーサイズ (ビット) およびシステムデフォルトに設定される EC キーサイズ (ビット) を残して下さい。
- オペレーションに関してはによって、入ります未来へ少なくとも 1 時間である日時に完了します。



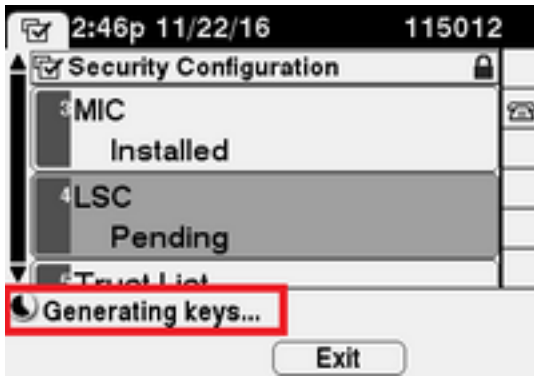


コンフィギュレーション変更を保存し、そして構成を適用して下さい。

電話の LSC ステータスはイメージに示すように保留中に変更します。



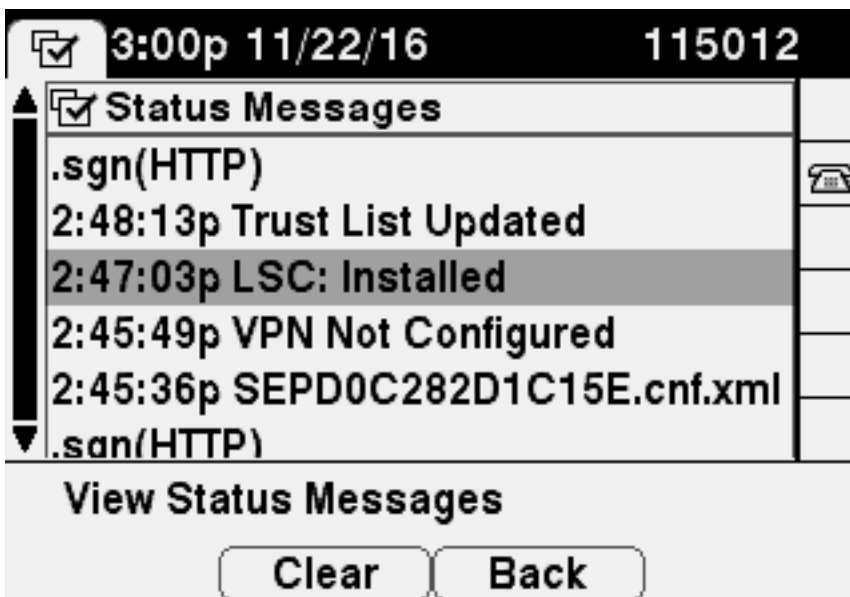
電話はイメージに示すようにキーを生成します。



リセットが完了する時電話リセット、および、イメージに示すようにインストールされるへの電話 LSC ステータス 変更。



これはまたイメージに示すように電話の目に見える下ステータスメッセージです。



## 確認

このセクションでは、設定が正常に機能していることを確認します。

複数の電話の LSC 認証インストールを確認するために、[Cisco Unified Communications Manager のためにセキュリティガイドの生成する CAPF 報告書節を、リリース 11.0\(1\) 参照して下さい。](#) また、[LSC ステータスまたは認証文字列](#) プロシージャによって検索電話を使用して CUCM 管理 Web インターフェイス内の同じデータを表示することができます。

電話にインストールされる LSC 証明書のコピーを入手するために [Cisco IP phones article から証明書を取得する方法](#)を参照して下さい。

## トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

### 有効な CAPF サーバ無し

LSC はインストールしません。電話のステータスメッセージは**有効な CAPF サーバがない**ことを示します。これは ITL ファイルに CAPF エントリがないことを示します。CAPF サービスがアクティブになった確認し、次に TFTP サービスをことを再起動して下さい。最新の ITL ファイルを取るために再始動が、電話をリセットした含まれ次に証明書 オペレーションを再試行する後 ITL ファイルが CAPF 証明書がことを確認して下さい。ホスト名として電話のセキュリティ設定メニュー ディスプレイの CAPF Server エントリ-または完全修飾ドメイン ネームは、電話をできません IP アドレスにエントリを解決確認します。

### LSC: 接続に失敗しました。

LSC はインストールしません。電話のステータスメッセージは **LSC を示します: 接続は失敗しました。** これはこれらの状態の 1 つを示すかもしれません:

- ITL ファイルの CAPF 証明書と現在の証明書間のミスマッチは、CAPF サービス使用中です。
  - CAPF サービスは停止するか、または無効になります。
  - 電話はネットワーク上の CAPF サービスに達することができません。

CAPF サービスがアクティブになり、CAPF サービスを、再始動 TFTP サービス clusterwide 再開始、最新の ITL ファイルを取るために電話をリセットし次に証明書 オペレーションを再試行することを確認して下さい。問題が持続する場合、電話および CUCM パブリッシャからのパケットキャプチャを奪取し、ポート 3804 に双方向通信があるかどうか見るために、デフォルト CAPF サービス ポート分析して下さい。そうでなかったら、ネットワーク上の問題があるかもしれません。

### LSC: Failed ( 故障 )

LSC はインストールしません。電話のステータスメッセージは **LSC を示します: 失敗しました。** 電話 設定 Web ページは **証明書 オペレーション ステータス** を表示します: **アップグレードは失敗しました: ユーザ 開始された要求遅く/Timeout。** これはオペレーションが時間と日付までに以前切れるか、またはある完了することを示します。未来へ少なくとも 1 時間である入り、次に証明書 オペレーションを再試行して下さい日時に。

## 関連情報

これらの文書は AnyConnect VPN クライアント 認証および 802.1X 認証にコンテキストの LSCs

の使用で詳細を提供します。

- [AnyConnect VPN 電話 - IP Phone、ASA、および CUCM のトラブルシューティング](#)
- [Identity-Based Networking Services : IEEE によって 802.1X 有効にされる ネットワーク配備およびコンフィギュレーション ガイドの IP テレフォニー](#)

また LSC 証明書がサードパーティによって認証局 ( CA ) 直接署名される高度タイプには LSC 設定が、ない CAPF 証明書あります。

詳細については、参照して下さい: [CUCM サードパーティ CA 署名済み LSC の作成およびインポートの設定例](#)

- [テクニカル サポートとドキュメント - Cisco Systems](#)