

CUCM 電話認証 (LSC/MIC) のための Q.A

目次

[概要](#)

[電話認証のための一般的な使用とは何か。](#)

[/アップグレードするための CAPF と電話間、削除するか、または解決しますインストール
Trasnsport 層 セキュリティ \(TLS \) 接続のための CallManager と電話間](#)

[802.1X 認証のための電話と認証サーバ間](#)

[VPN のための電話と Cisco 適応性があるセキュリティ アプライアンス モデル \(ASA \) 間の認証
ベースの認証に関しては](#)

[LSC および MIC が時接続に LSC か MIC を明示的に選択する、あらゆる方法ありますか。](#)

[原因は何を新しいクラスタに移動すると LSC インストール済み電話保護されたプロファイルの登録
されていませんか。](#)

[電話がそれを認証されたか、または暗号化された保護されたプロファイルを使用して登録されて
いて得ることができるようにインストールされる LSC があることを必要としますか。](#)

[認証されることは必須ことそれぞれデバイスセキュリティ プロファイルのデバイスセキュリティ
モードまたは暗号化された/アップグレード/削除インストールするために LSC ですか。](#)

[それは必須電話に LSC をインストールするミックス モードにあるクラスタですか。](#)

[そこに LSC においての問題すぐにテストする方法電話によって使用されますか。](#)

[トラブルシューティングのための電話認証を得る方法か。](#)

[電話の LSC か MIC 使用された確立するが CallManager の TLS 接続である場合パケットキャプ
チャから確認する方法か。](#)

[認証モードの重要性とは認証局 \(CA \) プロキシ 機能 \(CAPF \) 情報の下に何か。 CUCM と電話
間の TLS 接続のための重要性か。](#)

[CAPF 認証の後で考えるべき電話のための基本 LSC オペレーションとは何再生されたとか。](#)

[CallManager の TLS 接続](#)

[CAPF 信頼の LSC オペレーション](#)

[802.1X 認証のための電話と認証サーバ間](#)

[ASA と電話間](#)

[関連情報](#)

概要

この資料はいくつかの Cisco Unified Communications Manager (CUCM) 電話認証のための質疑
応答を取り扱っています。 電話認証の速いビューはここにあります。

製造業者インストール済み認証 (MIC) :

名前が示すと同時に、電話は MIC とプレインストールされ、これは管理者によって削除され/修
正することができません。 CA SHA2 を製造する認証局 (CA) 認証 CAP-RTP-001、CAP-RTP-
002、Cisco_Manufacturing_CA および Cisco は CUCM で MIC を信頼するためにプレインスト
ールされます。 MIC はできますか。 t は有効性が生成されるに関して MIC CA 傾斜としてあれば切
れれば使用されます、

ローカルで固有の認証 (LSC) :

LSC は Cisco Unified Communications Manager 認証局 プロキシ 機能 (CAPF) プライベートキーによって署名する Cisco IP Phone のための公開キーを所有しています。それは電話でデフォルトでインストールされていません。管理者は LSC を完全な制御をコントロールします。CAPF CA 認証は電話に必要とされて時はいつでも次々とできます新しい LSC を発行再生することができます。

電話認証のための一般的な使用とは何か。

電話認証のためのいくつかの一般的な使用はここにあります

/アップグレードするための CAPF と電話間、削除するか、または解決しますインストール

確立します電話で CAPF/アップグレードを用いる接続をインストールするか、削除するか、または認証を解決するために電話をかけて下さい。電話 Certificate が既存の認証 (LSC への優位) によってへのまたは既存の認証 (MIC への優位) によって設定される認証局 (CA) プロキシ機能 (CAPF) 情報の下で CAPF の接続をとき認証モード確立するのに使用されています。

既存の認証 (LSC への優位) によって: 電話は LSC を CAPF と認証するのに使用します。それは LSC がインストールされていない場合 MIC を使用します。インストールは原因「無効 LSC」と使用された認証においての問題がある場合失敗します。例は、LSC のための署名された CA CAPF 信頼で利用できません。他の認証方式を使用してまたはそのような失敗例のためのヌルストリングによって認証モードをアップデートして下さい。

既存の認証 (MIC への優位) によって: 電話は MIC を CAPF と認証するのに使用します。

Transport 層 セキュリティ (TLS) 接続のための CallManager と電話間

電話は LSC か MIC を CallManager の TLS 接続を確立するのに使用します。CallManager は CallManager 信頼のチェックによる電話によって示された Certificate を検証します。それぞれ CAPF 認証は LSC および Cisco 製造 CA のために CallManager 信頼で利用可能でなければなりません。MIC のための s。

802.1X 認証のための電話と認証サーバ間

CAPF/Manufacturing CA 証明書は Cisco Secure Access Control Server (ACS) または Identity Services Engine (ISE) のような認証サーバにアップロードされます。認証サーバはアップロードされた認証を時それ提供認証電話を認証するのに使用します (LSC か MIC) 。

VPN のための電話と Cisco 適応性があるセキュリティ アプライアンス モデル (ASA) 間の認証ベースの認証に関しては

CAPF/Manufacture CA 証明書は ASA で信頼電話現在の LIC/MIC がそのチェックによって、ASA それを検証するとき、アップロードされます。

LSC および MIC が時接続に LSC か MIC を明示的に選択する、

あらゆる方法ありますか。

接続にかどうか LSC が MIC 選択するオプション無し。LSC がインストールされている場合、電話は LSC を使用します。電話は LSC がインストールされていない場合 MIC を使用します。

LSC がない場合の Console エントリ:

SECD: - PXY_NO_LSC: LSC はのための[SCCP]、MIC を試みません

LSC がある場合の Console エントリ:

SECD: - PXY_CERT_CIPHER: [SCCP]、[TLSv1]、証明書[LSC]

LSC または MIC の選択は CAPF と電話/でアップグレードするか間でだけ可能性のある、削除するか、または解決しますインストール。

原因は何を新しいクラスタに移動すると LSC インストール済み電話保護されたプロファイルの登録されていませんか。

これは電話のために既に古いクラスタからの LSC を持っているそれら起こる場合があります。MIC および LSC が両方時、LSC が TLS 接続を確立するのに使用されています。TLS 新しい CUCM doesn't 以来確立することができませんか。t に CallManager 信頼でこの LSC のための CA があります。

コンソール ログはどの認証が TLS を確立するのに使用されているか示します。エントリの下で LSC が使用されることを示します。

3469 ない 00:01:31.935298 SECD: - PXY_CERT_CIPHER: [SCCP]、[TLSv1]、証明書[LSC]、暗号 [AES256-SHA:AES128-SHA]

SSL3_Alert とのか。未知 CA か。コンソール ログのそのような壊れるケースのため:-

3486 ERR 00:01:31.938954 SECD: -STATE_SSL3_ALERT: SSL3 アラート[読まれる]: [致命的]: [未知 CA]

この問題を解決する方法の 1 つはありまして、電話を非を使用して登録されていて得ますか。セキュア プロファイルはそれから既存の LSC を削除します。LSC を新しいクラスタからインストールしそして保護されたプロファイルを使用して電話を登録して下さい。それはまた可能性のある LSC をインストールしないで MIC を使用して登録されている保護されたプロファイルの電話があるためにです。

電話がそれを認証されたか、または暗号化された保護されたプロファイルを使用して登録されていて得ることができるようにインストールされる LSC があることを必要としますか。

いいえ。LSC がインストールされていない場合、電話は MIC を CUCM への TLS 接続を確立するのに使用します。

4878 WRN 15:47:34.756063 SECD: - PXY_NO_LSC: LSC 無しのための[SCCP]、試み MIC。

認証されることは必須ことそれぞれデバイスセキュリティ プロファイルのデバイスセキュリティ モードまたは暗号化された/アップグレード/削除インストールするために LSC ですか。

それはデフォルトの基準値非セキュア プロファイルを使用してデバイスセキュリティでモードが非セキュアであるところに必須、それ余りにすることができますではないです。

それは必須電話に LSC をインストールするミックス モードにあるクラスタですか。

それは必須ではないです。LSC インストール/削除は時でさえ非セキュアのクラスタ セキュリティモードすることができます。

そこに LSC においての問題すぐにテストする方法電話によって使用されますか。

電話管理者ページへ行くことによって電話の 1 の LSC を削除して下さい。これは MIC を使用するために電話を強制します。すべてが LSC をうまく MIC とそれからトラブルシューティング続行すれば。

トラブルシューティングのための電話認証を得る方法か。

デバイス/電話の下で解決するために認証 オペレーションを設定して下さい。ヒット保存はそれから構成を適用します。認証 オペレーション ステータスを成功を解決するために見るために待つして下さい。実時間監視 ツール (RTMT) から Cisco 認証局 プロキシ 機能ログを集めて下さい。それは電話からの認証が含まれています。

電話の LSC が MIC 使用された確立するが CallManager の TLS 接続である場合パケットキャプチャから確認する方法か。

電話再始動をカバーしているパケットキャプチャを集めて下さい。

認証を、Client 鍵 交換メッセージ チェックして下さい。IP Phone から送信される 認証を確認して下さい。

例 LSC:

LSC に関しては、CAPF CN は発行元 フィールドで見られます。それぞれ CAPF ルートは CallManager 信頼にあるなります。

```
223 _ 10.106.104.243 10.106.104.211 TLSv1 1514 Certificate, Client Key Exchange
224 _ 10.106.104.243 10.106.104.211 TLSv1 145 Certificate Verify
* issuer: rdnSequence (0)
  * rdnSequence: 6 items (id-at-localityName=Bangalore,id-at-stateOrProvinceName=Karnataka,id-at-commonName=CAPF-a6d4c572,
```

例 MIC:

MIC に関しては、発行元 フィールドの CA を製造する Cisco。それぞれルートCA は CallManager 信頼にあるなります。

396 ...	10.106.104.243	10.106.104.211	TLSv1	1514 Certificate, Client Key Exchange
397 ...	10.106.104.243	10.106.104.211	TLSv1	385 Certificate Verify

```
serialNumber: 0x75a85f6e0000000015d
> signature (sha256WithRSAEncryption)
+ issuer: rdnSequence (0)
  + rdnSequence: 2 items (id-at-commonName=Cisco Manufacturing CA SHA2,id-at-organizationName=Cisco)
```

認証モードの重要性とは認証局 (CA) プロキシ 機能 (CAPF) 情報の下に何か。CUCM と電話間の TLS 接続のための重要性か。

それはだけ//でオペレーションを削除し、のための電話と CAPF 間の認証方式解決しますアップグレード インストール。それ doesn か。t に CUCM と電話間の TLS 接続のための重要性があります。

CAPF 認証の後で考えるべき電話のための基本 LSC オペレーションとは何再生されたとか。

このセクションは LSC を発行するのにオフ・ライン CA が使用されていないアイドル状態のシナリオをカバーします。

CallManager の TLS 接続

CallManager 信頼から前の CAPF 認証を削除する前に電話で新しい LSC をインストールするために確認して下さい。CallManagerサービスの再始動に先行している前の CAPF 認証を削除してそれにこの CAPF 認証によって発行される LSC がある電話に登録問題を引き起こして下さい。

CAPF 信頼の LSC オペレーション

CAPF 信頼から前の CAPF 認証を削除する前に電話で新しい LSC をインストールするために確認して下さい。既存の認証 (LSC への優位) による認証モードを使用してインストール/削除のような LSC オペレーションはそれらにこの CAPF 認証によって発行される LSC がある電話のためのエラー 無効 LSC と失敗します。

802.1X 認証のための電話と認証サーバ間

アップロードされる新しい CAPF 認証および電話が LSC を新しい CAPF によって発行されて得るまで認証サーバから前の CAPF 認証を削除しないために確認して下さい。

ASA と電話間

電話が ASA に新しい LSC およびアップロードされた新しい CAPF CA 認証を得るまで ASA から前の CAPF 認証を削除しないために確認して下さい。

CAPF 認証を再生するために続かれるべきステップについては[認証再生成](#)を参照して下さい。

関連情報

- [Cisco IP Phone 認証およびセキュアコミュニケーション](#)
- [802.1X 設計の指針のための IP テレフォニー](#)
- [Cisco Unified Communications Manager セキュリティ ガイド](#)