Unified Communications Manager バージョン 10.0(1) における ITL の機能拡張

目次

概要

この資料は識別信頼リスト（ITL）ファイル統一された IP フォンのバルク リセットを on Cisco 有効に する Cisco Unified Communications Manager （CUCM）バージョン 10.0(1)で新しい 機能を説明していたものです。 バルク ITL リセット 機能は電話がもはや ITL ファイル署名者を信頼しないし、また TFTPサービスによってまたは信頼確認サービス（TV）の使用をローカルで与えられる ITL ファイルを認証できないとき使用されます。

背景説明

リセット ITL かさ張る機能はファイルこれらのステップの 1 つまたは IP 電話と CUCM サーバ間の信頼を再確立するために多数を実行する必要を防ぎます。

- バックアップからの復元電話が信頼する古い ITL ファイルをアップロードするため
- 別の TFTPサーバを使用するために電話を変更して下さい
- Settings メニューによって電話から ITL ファイルを手動で削除して下さい
- ファクトリは ITL を消すためアクセスが無効であるようにイベント設定の電話をリセットしました

この機能はクラスタの間で電話を移動するように意図されていません; そのタスクのために、CUCM 8 および ITL ファイルとクラスタの間で IP フォンを移行すること に説明があるメソッドの 1 つを使用して下さい。 それらが信頼ポイントを失ったらしか ITL リセット オペレーションが IP 電話と CUCM クラスタ間の信頼を再確立しないのに使用されています。

この資料でカバーされない CUCM バージョン 10.0(1)で利用可能 なもう一つのセキュリティ関連の機能は Tokenless Certficate 信頼リスト（CTL）です。 Tokenless CTL は CUCM サーバおよびエンドポイントの暗号化を有効に するために使用されるソフトウェア トークンとハードウェア USB セキュリティ トークンを取り替えます。 その他の情報に関しては、IP Phone セキュリティおよび CTL（証明書信頼リスト）資料を参照して下さい。

ITL ファイルのその他の情報およびセキュリティは通信マネージャ セキュリティでデフォルトでデフォルトでおよび ITL オペレーションおよびトラブルシューティングに関する文書見つけることができます。

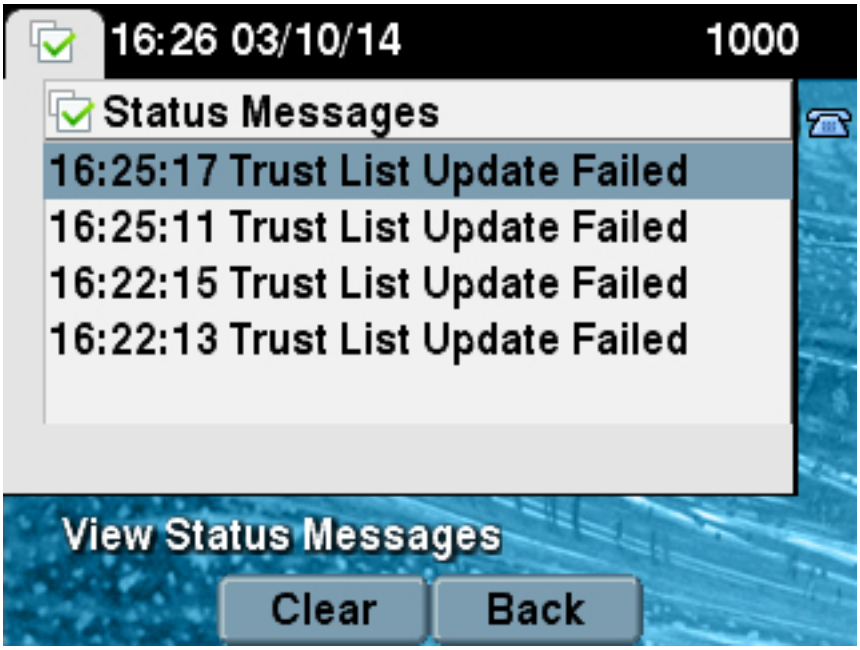
問題の症状

電話が**ロックされたのか信頼できない状態**にあるとき、TFTPサービスによって提供される ITL ファイルか TFTP 設定を受け入れません。 TFTP コンフィギュレーション ファイルで含まれているどのコンフィギュレーション変更でも電話に加えられません。 TFTP コンフィギュレーション ファイルで含まれている設定の例は次のとおりです:

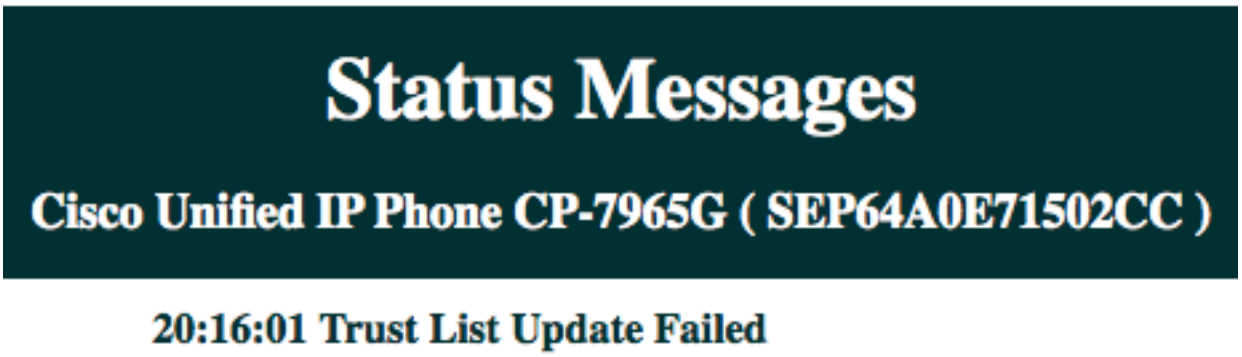
- 設定アクセス
- Web アクセス
- セキュア シェル（SSH）アクセス
- PCポートへのスイッチ型ポートアナライザ（SPAN）

これらの設定のうちのどれかが CCM 管理者ページの電話および変更される場合、電話がリセットされた後、変更のために、電話 TFTPサーバを信頼しないかもしれません実施されないで下さい。 もう一つのよくみられる症状は社内 ディレクトリか他の電話サービスにアクセスするとき、メッセージ **ホスト見つけられなかった**ディスプレイあります。 電話がロックされたのか信頼できない状態にあることを確認するために、電話からの電話ステータスメッセージ自体か電話 Webページをかどうか**信頼リスト アップデート 失敗通知メッセージ** ディスプレイ確認して下さい。 **ITL アップデート 失敗通知メッセージは**電流 ITL が付いている信頼リストを認証しなかった、TV とそれを認証しなかったので電話がロックされたのか信頼できない状態にあることインジケータです。

信頼リスト アップデート 失敗通知メッセージは電話自体から**設定 > ステータス > ステータスメッセージ**にナビゲート する場合見られる場合があります:



信頼リスト アップデート 失敗通知メッセージはまたここに示されているように**ステータスメッセージ**からの電話 Webページから見られる場合があります:



ソリューション-バルク ITL リセット

CUCM バージョン 10.0(1)は電話と CUCM サーバ間の信頼を再確立するために使用できる追加キーを使用します。 この New 鍵は ITL 回復キーです。 ITL リカバリ キーはインストールかアップグレードの間に作成されます。 このリカバリ キーはホスト名が変更すると、DNS 変更します変更しません、または電話がもはやコンフィギュレーション ファイルの署名者を信頼しない状態に得る問題を引き起こす原因となるかもしれない他の変更は実行された。

新しい **utils itl リセット** CLI コマンドは電話が**信頼リスト アップデート 失敗通知メッセージが**見られる状態にとき電話間の信頼と CUCM の TFTPサービスを再確立するために使用することができます。 **utils itl reset コマンド**:

1. パブリッシャ ノードからの電流 ITL ファイルを奪取 し、ITL ファイルのシグ二チャを除去し、ITL リカバリ プライベートキーと ITL ファイルのコンテンツに再度署名します。
2. 自動的にクラスタの TFTP アクティブなノードすべての TFTP ディレクトリに新しい ITL ファイルをコピーします。
3. 自動的に TFTP が動作する各ノードの TFTP サービスを再開します。

管理者はそれから電話すべてをリセットする必要があります。 リセットにより TFTPサーバから電話は起動します ITL ファイルを請求します、電話が **callmanager.pem プライベートキー**の代りに ITLRecovery キーによって署名する受け取る ITL ファイル。 リセットされる ITL を実行する 2 つのオプションがあります: utilsitl **リセット localkey および** utilsitl **リセット remotekey。** ITL reset コマンドはパブリッシャからしか実行することができません。 サブスクライバからリセットされる ITL を発行する場合 Thisis という結果に**ないパブリッシャ ノード メッセージ**終ります。 各コマンドの例は次の セクションで詳述されます。

ローカル リカバリ キーの ITLRecovery

localkey オプションはパブリッシャ ハード ドライブの ITLRecovery.p12 ファイルに含まれている ITL リカバリ プライベートキーをように新しい ITL ファイル署名者使用します。

```
admin:utils itl reset localkey
Enter CCM Administrator password :

Locating active Tftp servers in the cluster.....

Following is the list of Active tftp servers in the cluster
```

```
['test10pub', 'test10sub']
The reset ITL file was generated successfully


Transferring new reset ITL file to the TFTP server nodes in the cluster.........

Restarting Cisco Tftp service on host test10pub
Cisco Tftp service restarted on host test10pub
Successfully transferred reset ITL to node test10sub

Restarting Cisco Tftp service on host test10sub
Cisco Tftp service restarted on host test10sub
```

リモート リカバリ キーの ITLRecovery

remotekey オプションは ITLRecovery.p12 ファイルが規定 されるために保存された外部 SFTP サーバを可能にします。

```
admin:utils itl reset remotekey joemar2-server.cisco.com joemar2
/home/joemar2/ITLRecovery.p12
Enter Sftp password :Processing token in else 0 tac
coutn is 1
Processing token in else 0 tac
coutn is 1



Enter CCM Administrator password :

Locating active Tftp servers in the cluster.....

Following is the list of Active tftp servers in the cluster

['test10pub', 'test10sub']
The reset ITL file was generated successfully


Transferring new reset ITL file to the TFTP server nodes in the cluster.........

Restarting Cisco Tftp service on host test10pub
Cisco Tftp service restarted on host test10pub
Successfully transferred reset ITL to node test10sub

Restarting Cisco Tftp service on host test10sub
Cisco Tftp service restarted on host test10sub
```

> **注:** ITL リセットが remotekey オプションとされる場合、パブリッシャの localkey は（ディスク ファイルで） remotekey と取り替えられます。

「itl」コマンドで現在の署名者が示すことを確認して下さい

ITL reset コマンドを発行する前に**提示 itl** コマンドで ITL ファイルを表示すれば、ITL が **ITLRECOVERY_ *< publisher_hostname - > エントリ***含まれていることを示します。 各 ITL ファイルはクラスタのあらゆる TFTPサーバによって動作されるパブリッシャからのこの ITL リカバリ エントリが含まれています。 **提示 itl** コマンドの出力はこの例のパブリッシャから奪取 されます。 ITL に署名するために使用されるトークンは太字にあります:

```
admin:show itl
```

The checksum value of the ITL file:
b331e5bfb450926e816be37f2d8c24a2(MD5)
9d7da73d16c1501b4d27dc1ed79211f390659982(SHA1)

Length of ITL file: 5302
The ITL File was last modified on Wed Feb 26 10:24:27 PST 2014

Parse ITL File

Version: 1.2
HeaderLength: 324 (BYTES)

BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
3 SIGNERID 2 139
4 SIGNERNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
5 SERIALNUMBER 16 61:40:52:E9:1E:E9:7C:77:9B:7B:5E:81:0A:B1:46:A5
6 CANAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
7 SIGNATUREINFO 2 15
8 DIGESTALGORTITHM 1
9 SIGNATUREALGOINFO 2 8
10 SIGNATUREALGORTITHM 1
11 SIGNATUREMODULUS 1
12 SIGNATURE 128
8f d4 0 cb a8 23 bc b0
f 75 69 9e 25 d1 9b 24
49 6 ae d0 68 18 f6 4
52 f8 1d 27 7 95 bc 94
d7 5c 36 55 8d 89 ad f4
88 0 d7 d0 db da b5 98
12 a2 6f 2e 6a be 9a dd
da 38 df 4f 4c 37 3e f6
ec 5f 53 bf 4b a9 43 76
35 c5 ac 56 e2 5b 1b 96
df 83 62 45 f5 6d 0 2f
c d1 b8 49 88 8d 65 b4
34 e4 7c 67 5 3f 7 59
b6 98 16 35 69 79 8f 5f
20 f0 42 5b 9b 56 32 2b
c0 b7 1a 1e 83 c9 58 b
14 FILENAME 12
15 TIMESTAMP 4

ITL Record #:1

BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1115
2 DNSNAME 2
3 SUBJECTNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 61:40:52:E9:1E:E9:7C:77:9B:7B:5E:81:0A:B1:46:A5
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 684 01 9C 4C 3D 27 D7 4D 82 CB B1 84 84 D4 2A 63 9F 71 78 BE A9
(SHA1 Hash HEX)
This etoken was used to sign the ITL file.

ITL Record #:2

BYTEPOS TAG LENGTH VALUE

```
------- --- ------ -----
1 RECORDLENGTH 2 1115
2 DNSNAME 2
3 SUBJECTNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 TFTP
5 ISSUERNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 61:40:52:E9:1E:E9:7C:77:9B:7B:5E:81:0A:B1:46:A5
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 684 01 9C 4C 3D 27 D7 4D 82 CB B1 84 84 D4 2A 63 9F 71 78 BE A9
(SHA1 Hash HEX)
ITL Record #:3
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 439
2 DNSNAME 2
3 SUBJECTNAME 49 CN=CAPF-75638ad9;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 CAPF
5 ISSUERNAME 49 CN=CAPF-75638ad9;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 42:BF:37:77:9B:16:AF:1C:D2:30:88:C2:17:24:9D:AA
7 PUBLICKEY 140
8 SIGNATURE 128
11 CERTHASH 20 BB C3 4A 1D DE 17 39 C5 36 1A 15 6B F0 65 FE BE D1 E6 19 03
12 HASH ALGORITHM 1 SHA-1

ITL Record #:4
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 455
2 DNSNAME 2
3 SUBJECTNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 76:59:84:D8:B7:30:60:63:36:E5:C7:B6:A7:DD:B9:D6
7 PUBLICKEY 140
8 SIGNATURE 128
11 CERTHASH 20 7A BF CE B6 BE E2 06 02 74 D9 EB AE 58 48 52 93 7A 1E A5 55
12 HASH ALGORITHM 1 SHA-1

ITL Record #:5
----
BYTEPOS TAG LENGTH VALUE


------- --- ------ -----
1 RECORDLENGTH 2 1141
2 DNSNAME 2
3 SUBJECTNAME 66 CN=ITLRECOVERY_test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;
ST=nc;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 66 CN=ITLRECOVERY_test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;
ST=nc;C=US
6 SERIALNUMBER 16 6E:3F:65:C2:97:B3:E0:1F:E7:42:81:AB:52:CC:55:DC
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 692 CD C7 4A 39 87 87 52 FA B0 89 0C 28 AB CB 36 32 EB 87 16 DC
(SHA1 Hash HEX)
```
This etoken was not used to sign the ITL file.

```
ITL Record #:6
----
BYTEPOS TAG LENGTH VALUE
```

```
------- --- ------ -----
1 RECORDLENGTH 2 713
2 DNSNAME 2
3 SUBJECTNAME 57 CN=test10sub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 57 CN=test10sub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 67:D1:A1:9E:F8:AB:91:E6:C0:A6:10:35:26:30:EE:02
7 PUBLICKEY 270
8 SIGNATURE 256
11 CERTHASH 20 AF 28 89 16 F9 94 E6 62 A3 65 C2 88 3B 94 08 1C 66 7C 49 C9
12 HASH ALGORITHM 1 SHA-1

The ITL file was verified successfully.
```

ITLRecovery キーが使用されることを確認して下さい

ITL リセットを行った後**提示 itl** コマンドで ITL ファイルを表示すれば、ITLRecovery エントリがここに示されているように ITL に署名したことを示します。 ITLRecovery は ITL に再度署名するために TFTP **callmanager.pem** が認証は使用されますその時点で TFTP が再起動するまで ITL の署名者に残ります。

```
admin:show itl
The checksum value of the ITL file:
c847df047cf5822c1ed6cf376796653d(MD5)
3440f94f9252e243c99506b4bd33ea28ec654dab(SHA1)


Length of ITL file: 5322
The ITL File was last modified on Wed Feb 26 10:34:46 PST 2014<

Parse ITL File
----------------

Version: 1.2
HeaderLength: 344 (BYTES)

BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
3 SIGNERID 2 157
4 SIGNERNAME 66 CN=ITLRECOVERY_test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
5 SERIALNUMBER 16 6E:3F:65:C2:97:B3:E0:1F:E7:42:81:AB:52:CC:55:DC
6 CANAME 66 CN=ITLRECOVERY_test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
7 SIGNATUREINFO 2 15
8 DIGESTALGORTITHM 1
9 SIGNATUREALGOINFO 2 8
10 SIGNATUREALGORTITHM 1
11 SIGNATUREMODULUS 1
12 SIGNATURE 128
58 ff ed a ea 1b 9a c4
e 75 f0 2b 24 ce 58 bd
6e 49 ec 80 23 85 4d 18
8b d0 f3 85 29 4b 22 8f
b1 c2 7e 68 ee e6 5b 4d
f8 2e e4 a1 e2 15 8c 3e
97 c3 f0 1d c0 e 6 1b
fc d2 f3 2e 89 a0 77 19
5c 11 84 18 8a cb ce 2f
5d 91 21 57 88 2c ed 92
a5 8f f7 c 0 c1 c4 63
28 3d a3 78 dd 42 f0 af
9d f1 42 5e 35 3c bc ae
c 3 df 89 9 f9 ac 77
```

```
60 11 1f 84 f5 83 d0 cc
14 FILENAME 12
15 TIMESTAMP 4

ITL Record #:1
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1115
2 DNSNAME 2
3 SUBJECTNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 61:40:52:E9:1E:E9:7C:77:9B:7B:5E:81:0A:B1:46:A5
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 684 01 9C 4C 3D 27 D7 4D 82 CB B1 84 84 D4 2A 63 9F 71 78 BE A9
(SHA1 Hash HEX)
```
This etoken was not used to sign the ITL file.
```
ITL Record #:2
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1115
2 DNSNAME 2
3 SUBJECTNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 TFTP
5 ISSUERNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 61:40:52:E9:1E:E9:7C:77:9B:7B:5E:81:0A:B1:46:A5
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 684 01 9C 4C 3D 27 D7 4D 82 CB B1 84 84 D4 2A 63 9F 71 78 BE A9
(SHA1 Hash HEX)

ITL Record #:3
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 439
2 DNSNAME 2
3 SUBJECTNAME 49 CN=CAPF-75638ad9;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 CAPF
5 ISSUERNAME 49 CN=CAPF-75638ad9;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 42:BF:37:77:9B:16:AF:1C:D2:30:88:C2:17:24:9D:AA
7 PUBLICKEY 140
8 SIGNATURE 128
11 CERTHASH 20 BB C3 4A 1D DE 17 39 C5 36 1A 15 6B F0 65 FE BE D1 E6 19 03
12 HASH ALGORITHM 1 SHA-1

ITL Record #:4
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 455
2 DNSNAME 2
3 SUBJECTNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 76:59:84:D8:B7:30:60:63:36:E5:C7:B6:A7:DD:B9:D6
7 PUBLICKEY 140
8 SIGNATURE 128
11 CERTHASH 20 7A BF CE B6 BE E2 06 02 74 D9 EB AE 58 48 52 93 7A 1E A5 55
12 HASH ALGORITHM 1 SHA-1
```

```
ITL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1141
2 DNSNAME 2
3 SUBJECTNAME 66 CN=ITLRECOVERY_test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 66 CN=ITLRECOVERY_test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 6E:3F:65:C2:97:B3:E0:1F:E7:42:81:AB:52:CC:55:DC
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 692 CD C7 4A 39 87 87 52 FA B0 89 0C 28 AB CB 36 32 EB 87 16 DC
(SHA1 Hash HEX)
This etoken was used to sign the ITL file.

ITL Record #:6
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 713
2 DNSNAME 2
3 SUBJECTNAME 57 CN=test10sub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 57 CN=test10sub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US
6 SERIALNUMBER 16 67:D1:A1:9E:F8:AB:91:E6:C0:A6:10:35:26:30:EE:02
7 PUBLICKEY 270
8 SIGNATURE 256
11 CERTHASH 20 AF 28 89 16 F9 94 E6 62 A3 65 C2 88 3B 94 08 1C 66 7C 49 C9
12 HASH ALGORITHM 1 SHA-1

The ITL file was verified successfully.
```

信頼を失う電話の可能性を減少させる拡張

ITL リセット機能に加えて、CUCM バージョン 10.0(1)は電話は信頼できない状態を入力することを防ぐのを助ける管理者 機能が含まれています。 2 信頼は電話を持っていますです TV 認証（**TVS.pem) および** TFTP 認証（callmanager.pem) 指します。 1 CUCM サーバだけの、電話リセットはおよび起動時に最も簡単な環境**では**管理者が別のものの直後に callmanager.pemcertificate および TVS.pem 認証 1 を再生すれば信頼リスト **アップデート 失敗通知メッセージを**表示する。 CUCM から再生する ITL に含まれている認証による電話に送信される自動デバイス リセットと、電話は CUCM を信頼しない状態を入力することができます。

多重 認証が同時に再生するシナリオを防ぐのを助けるために（一般的にホスト名変更または DNS ドメイン名修正）、CUCM に今保持タイマーがあります。 認証が再生するとき、CUCM は管理者が前の認証再生成の 5 分以内の同じノードの別の認証を再生することを防ぎます。 このプロセスは電話を最初の認証を再生した上でリセットします次の認証が再生する前に登録されてバックアップであり。

どのに関係なく認証が最初に生成されるか、電話にファイルを認証するセカンダリ方式があります。 このプロセスについての追加詳細は通信マネージャ セキュリティでデフォルトでおよび ITL オペレーションおよびトラブルシューティング見つけることができます。

管理者は CLI から表示されるように前の認証再生成の 5 分以内の別の認証を再生することを CUCM がどこに防ぐかこの出力に状況に示されています:

```
admin:set cert regen CallManager
```

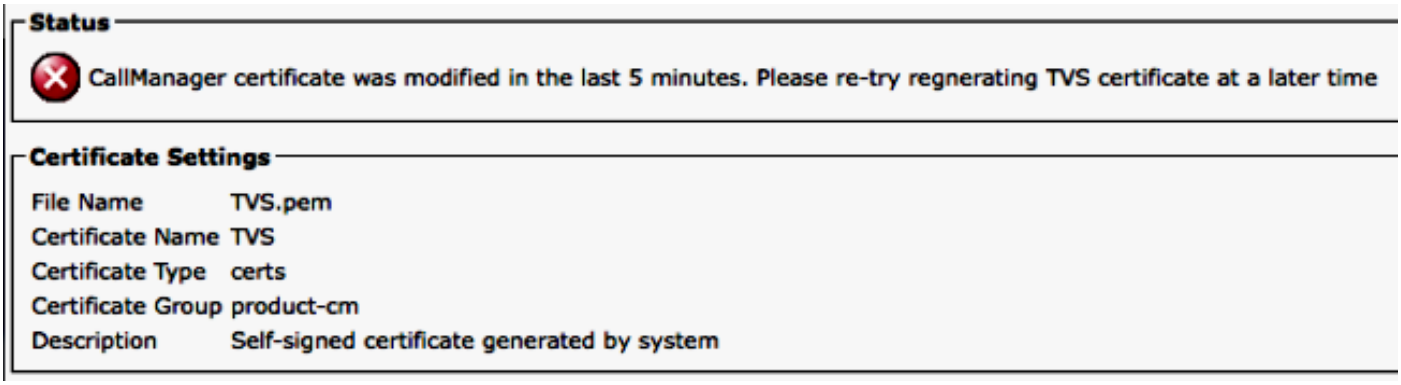
```
WARNING: This operation will overwrite any CA signed certificate
previously imported for CallManager
Proceed with regeneration (yes|no)? yes


Successfully Regenerated Certificate for CallManager.
Please do a backup of the server as soon as possible. Failure to do
so can stale the cluster in case of a crash.
You must restart services related to CallManager for the regenerated
certificates to become active.

admin:set cert regen TVS

CallManager certificate was modified in the last 5 minutes. Please re-try
regnerating TVS certificate at a later time
```

同じメッセージはここに示されているように Operating System （ OS ） 管理 ページから見られる場合があります:



パブリッシャ ITL リカバリ キーは各ノードに **ITLRecovery_** ***<node name>*** の Common Name （ CN ）に発行される ITLRecovery 自身の認証があるのに全体のクラスタによって使用中の唯一のものです。 パブリッシャ ITLRecovery キーは**提示 itl** コマンドから見られるように全体のクラスタのために ITL ファイルで使用される唯一のものです。 こういうわけで唯一の **ITLRecovery_ <*ホスト名*-** ITL ファイルで見られる ***> エントリは***ホスト名が含まれています-パブリッシャの…。

パブリッシャのホスト名が変更される場合、ITL の ITLRecovery エントリはパブリッシャの古いホスト名を示し続けます。 これは電話信頼に ITL リカバリを常に確認するために ITLRecovery ファイルが決して変更するべきではないので計画的にされます。

これはドメイン名が変更されるもときに適用します; オリジナルドメイン名は ITLRecovery エントリでリカバリ キーが変更しないようにするために表示されます。 5 年有効性が原因で切れる再生する必要がある必要がある時 ITLRecovery 認証があり、変更する唯一の時。

ITL 回復 keypairs は CLI か OS 管理 ページと再生することができます。 IP 電話は ITLRecovery 認証がパブリッシャまたはサブスクライバの何れかで再生するときリセットされません。 ITLRecovery 認証が再生したら、ITL ファイルは TFTPサービスが再起動するまでアップデートしません。 パブリッシャの ITLRecovery 認証再生成の後で、新しい認証との ITL ファイルの ITLRecovery エントリをアップデートするためにクラスタの TFTPサービスを実行する各ノードの TFTPサービスを再起動して下さい。 最後の段階は **System > Enterprise Parameters** からのすべてのデバイスをリセットし、すべてのデバイスに新しい ITL ファイルをダウンロードさせます ITLRecovery 新しい認証が含まれている Reset ボタンを使用することです。

ITL リカバリをバックアップして下さい

信頼できない状態を入力するとき ITL リカバリ キーが電話を回復 するために必要となります。 これが原因で、新しい実時間監視 ツール（RTMT）アラートは ITL リカバリ キーがバックアップされるまで生成された毎日です。 ディザスタ リカバリ システム（DR）バックアップはアラートを停止することを足りません。 ITL リカバリ キーを保存するためにバックアップが推奨されるがキーファイルの手動バックアップは同様に必要とされます。

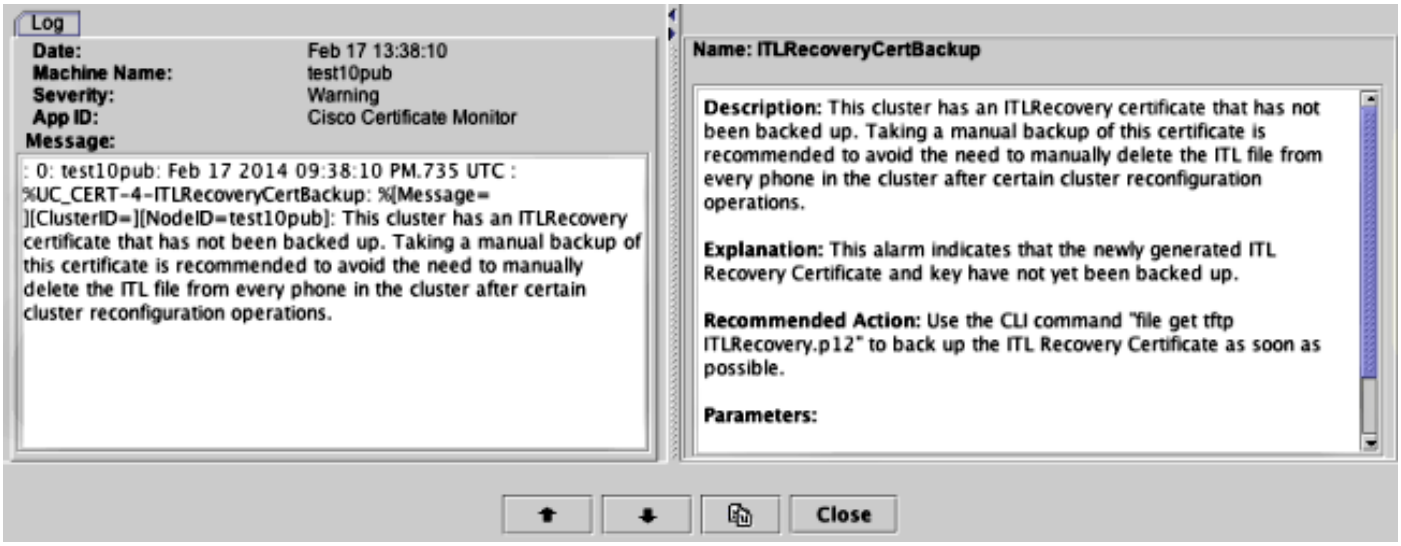
リカバリ キーを、ログインはパブリッシャの CLI にバックアップし、**ファイル名を**入力するために **tftp ITLRecovery.p12** コマンドを**得ます**。 SFTP サーバは必要ここに示されているようにファイルをに保存するためです。 Subscriber ノードに**見つけられないファイル**という結果に ITL 回復ファイルがありませんでしたり、従って**ファイルを**発行すればサブスクライバの **tftp ITLRecovery.p12** コマンドを、それ終ります**得ます**。

```
admin:file get tftp ITLRecovery.p12
Please wait while the system is gathering files info ...done.
Sub-directories were not traversed.
Number of files affected: 1
Total size in Bytes: 1709
Total size in Kbytes: 1.6689453
Would you like to proceed [y/n]? y
SFTP server IP: joemar2-server.cisco.com
SFTP server port [22]:
User ID: joemar2
Password: *************

Download directory: /home/joemar2/

The authenticity of host 'joemar2-server.cisco.com (172.18.172.254)' can't be
established.
RSA key fingerprint is 2c:8f:9b:b2:ff:f7:a6:31:61:1b:bc:95:cc:bc:ba:bd.
Are you sure you want to continue connecting (yes/no)? yes
.
Transfer completed.
Downloading file: /usr/local/cm/tftp/ITLRecovery.p12
```

ITLRecovery.p12 ファイルをバックアップするために手動バックアップが CLI から実行されたまで警告は CiscoSyslog （イベントビューアアプリケーションログ）でここに示されているように毎日印刷されます。 毎日電子メールはまた電子メール通知が OS 管理 ページから有効に なれば手動バックアップが、**セキュリティ > 認証 モニタ** 実行されたまで受信されるかもしれません。



DR バックアップが ITLRecovery が含まれている間、バックアップ ファイルがまたはバックアップから復元する必要なしで ITL ファイルをリセットするオプションを持つために失われるか、または破損すればまだ安全な位置で ITLRecovery.p12 ファイルを保存することを推奨します。 保存されるパブリッシャからの ITLRecovery.p12 ファイルがある場合またパブリッシャが使用のバッ

クアップなしで susbcriber からのデータベースを復元する、**utils itl リセット remotekey** オプションの ITL のリセットによって電話と CUCM サーバ間の信頼を再確立する DR Restore オプション再製されることを可能にします。

パブリッシャが再製されたら、クラスタ セキュリティパスワードは ITLRecovery.p12 ファイルがから奪取 された パブリッシャと同じ ITLRecovery.p12 ファイルがクラスタ セキュリティパスワードの基づいてパスワードとパスワードで保護されすのでであるはずであることを覚えていて下さい。 従って ITLRecovery.p12 ファイルはバックアップされなかったことを示すクラスタ セキュリティパスワードが変更されれば、RTMT アラートはリセットされ、新しい ITLRecovery.p12 ファイルが**ファイルと得る tftp ITLRecovery.p12** コマンドを保存されるまで毎日を引き起こします。

確認

バルク ITL リセット 機能は電話がインストールされる ITLRecovery エントリが含まれている ITL を備えている場合その時だけ動作します。 電話でインストールされる ITL ファイルが ITLRecovery エントリが含まれていることを確認するために、ITL ファイルのチェックサムを見つけるために TFTP サーバのそれぞれの CLI から**提示 itl** コマンドを入力して下さい。 **提示 itl** コマンドからの出力はチェックサムを表示するものです:

```
admin:show itl
The checksum value of the ITL file:
b331e5bfb450926e816be37f2d8c24a2(MD5)
9d7da73d16c1501b4d27dc1ed79211f390659982(SHA1)
```

チェックサムは各サーバに ITL ファイルで自身の **callmanager.pem 認証が**あるので各 TFTPサーバで異なっています。 電話でインストールされる ITL の ITL チェックサムは設定 **> Security 設定 > 信頼リスト**の下で、電話 Webページ、またはより新しいファームウェアを実行する電話によって報告される DeviceTLInfo アラームから電話の ITL 自体を表示する場合見つけることができます。

DeviceTLInfo アラームと CUCM にファームウェアのバージョン 9.4(1) またはそれ以降レポートを ITL の SHA1 ハッシュ送るほとんどの電話。 電話によって送信 される 情報は RTMT からのイベントビューアアプリケーションログで表示することができ、インストールされる ITLRecovery エントリが含まれている電流 ITL を備えていない電話を見つけるために TFTP サーバの ITL ハッシュの SHA1 ハッシュと比較されて電話は使用します。

警告

- CSCun18578 - ITL リセット localkey/remotekey はある特定の場合失敗します
- CSCun19112 - SFTP 認証不良型の ITL リセット remotekey エラー