تحسينات ITL لمدير الاتصالات الموحدة في الإصدار 10.0(1)

المحتويات

المقدمة

يصف هذا المستند ميزة جديدة في الإصدار 10.0(1) من (Cisco Unified Communications Manager (CUCM التي تتيح إعادة الضبط المجمعة لملفات قائمة أمان الهوية (ITL) على هواتف بروتوكول الإنترنت (IP) الموحدة من Cisco. يتم إستخدام ميزة إعادة تعيين ITL المجمع عندما لا تعود الهواتف تثق في الموقع الخاص بملف ITL ولا يمكنها أيضا مصادقة ملف ITL الذي توفره خدمة TFTP محليا أو باستخدام خدمة التحقق من الثقة (TVS).

الخلفية

تمنع القدرة على إعادة ضبط ملفات ITL مجمعة الحاجة إلى تنفيذ خطوة أو العديد من هذه الخطوات لإعادة إنشاء الثقة بين هواتف IP وخوادم CUCM.

- الاستعادة من نسخة إحتياطية لتحميل ملف ITL قديم تثق به الهواتف
- تغيير الهواتف لاستخدام خادم TFTP مختلف
- احذف ملف ITL يدويا من الهاتف من خلال قائمة الإعدادات
- إعادة ضبط الهاتف في المصنع في إعدادات الحدث بحيث يتم تعطيل الوصول من أجل مسح ITL

لا تهدف هذه الميزة إلى نقل الهواتف بين مجموعات البيانات؛ بالنسبة لهذه المهمة، أستخدم إحدى الطرق الموضحة في ترحيل هواتف IP بين المجموعات باستخدام ملفات CUCM 8 و ITL. لا تستخدم عملية إعادة ضبط سجل المعاملات الدولي إلا لإعادة بناء الثقة بين هواتف IP ومجموعة CUCM عندما تفقد نقاط الثقة الخاصة بها.

هناك ميزة أخرى متعلقة بالأمان متوفرة في الإصدار 10.0(1) من CUCM لا يغطيها هذا المستند وهي قائمة الثقة بدون رمز (CTL). تقوم قائمة التحكم في الوصول (CTL) غير المزورة باستبدال رموز أمان USB الخاصة بالأجهزة باستخدام رمز مميز للبرامج لتمكين التشفير على خوادم CUCM ونقاط النهاية. للحصول على معلومات إضافية، ارجع

إلى مستند أمان هاتف IP وقائمة الشهادات الموثوق بها CTL.

يمكن العثور بشكل افتراضي على معلومات إضافية حول ملفات ITL والأمان في أمان مدير الاتصالات بشكل افتراضي مستند تشغيل واستكشاف أخطاء ITL وإصلاحها.

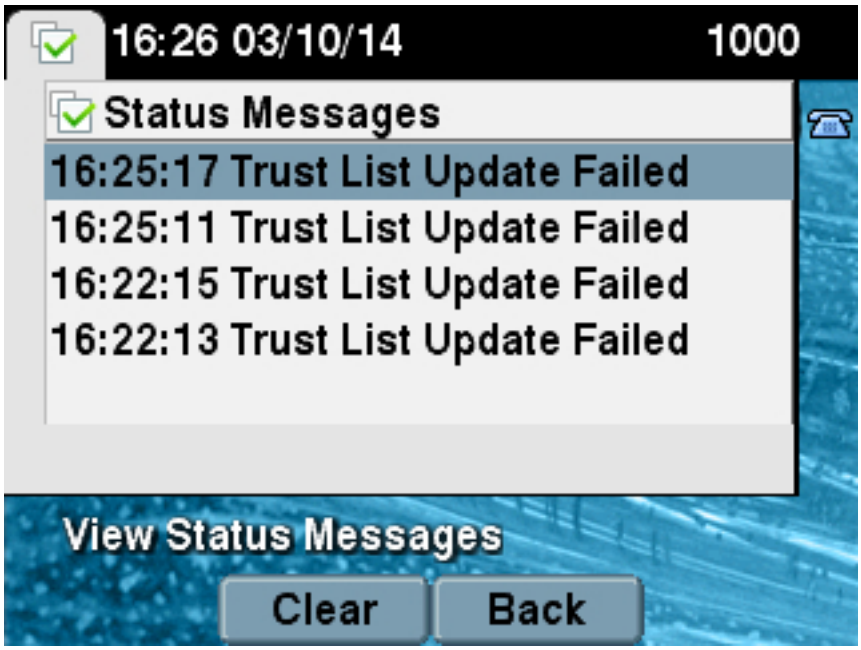
أعراض المشكلة

عندما تكون الهواتف في حالة **مؤمنة** أو **غير موثوق بها**، فإنها لا تقبل تكوين ملف ITL أو TFTP الذي توفره خدمة TFTP. لا يتم تطبيق أي تغيير تكوين في ملف تكوين TFTP على الهاتف. بعض الأمثلة على الإعدادات الموجودة في ملف تكوين TFTP هي:

- الوصول إلى الإعدادات
- الوصول إلى الويب
- الوصول الآمن إلى (Secure Shell (SSH
- محلل منفذ المحول (SPAN) إلى منفذ الكمبيوتر الشخصي

إذا تم تغيير أي من هذه الإعدادات لهاتف على صفحة إدارة CCM، وبعد إعادة تعيين الهاتف، لا تصبح التغييرات نافذة المفعول، قد لا يثق الهاتف بخادم TFTP. من الأعراض الأخرى الشائعة أنه عندما تقوم بالوصول إلى دليل الشركة أو خدمات الهاتف الأخرى، **لم يتم العثور على** عروض **لمضيف** الرسالة. للتحقق من أن الهاتف في حالة مؤمنة أو غير موثوق بها، تحقق من رسائل حالة الهاتف من الهاتف نفسه أو من صفحة ويب الهاتف لمعرفة ما إذا كان يتم عرض رسالة **فشل تحديث قائمة الثقة**. رسالة **فشل تحديث ITL** هي مؤشر على أن الهاتف في حالة مقفلة أو غير موثوق بها نظرا لفشله في مصادقة قائمة الثقة مع قائمة ITL الحالية الخاصة به وفشله في مصادقته باستخدام أجهزة التلفزيون.

يمكن مشاهدة رسالة **فشل تحديث قائمة الثقة** من الهاتف نفسه إذا قمت بالتنقل إلى **الإعدادات > الحالة > رسائل الحالة**:



يمكن أيضا مشاهدة رسالة **فشل تحديث قائمة الثقة** من صفحة ويب الهاتف من **رسائل الحالة** كما هو موضح هنا:

الحل - إعادة تعيين ITL المجمع

يستخدم CUCM الإصدار 10.0(1) مفتاح إضافي يمكن إستخدامه لإعادة تأسيس الثقة بين الهواتف وخوادم CUCM. هذا المفتاح الجديد هو مفتاح إسترداد ITL. يتم إنشاء مفتاح إسترداد ITL أثناء التثبيت أو الترقية. لا يتغير مفتاح الاسترداد هذا عند تغيير اسم المضيف أو تغيير DNS أو إجراء تغييرات أخرى قد تؤدي إلى حدوث مشاكل عندما تصل الهواتف إلى حالة لم تعد تثق فيها في الموقع الخاص بملفات التكوين الخاصة بها.

يمكن إستخدام أمر واجهة سطر الأوامر الجديد CLI لإعادة إنشاء الثقة بين الهاتف أو الهواتف وخدمة TFTP على CUCM عندما تكون الهواتف في حالة ظهور رسالة **فشل تحديث قائمة الثقة**. أمر **إعادة تعيين مستخدم** الإنترنت:

1. يأخذ ملف ITL الحالي من عقدة الناشر، يجرد توقيع ملف ITL، ويوقع محتويات ملف ITL مرة أخرى باستخدام المفتاح الخاص باسترداد ITL.
2. ينسخ ملف ITL الجديد تلقائيا إلى دلائل TFTP في كل عقد TFTP النشطة في نظام المجموعة.
3. يقوم بإعادة تشغيل خدمات TFTP تلقائيا على كل عقدة يعمل بها TFTP.

يجب على المسؤول إعادة ضبط جميع الهواتف. تتسبب عملية إعادة الضبط في أن تطلب الهواتف ملف ITL عند التمهيد من خادم TFTP، ويتم توقيع ملف ITL الذي يستلم الهاتف بواسطة مفتاح ITLRecovery بدلا من المفتاح الخاص **callManager.pem**. هناك خياران لتشغيل إعادة تعيين ITL: **إعادة تعيين مفتاح الإعدادات المحلية** في **كل مرة**، **وإعادة تعيين RemoteKey مرة أخرى**. يمكن تشغيل أمر إعادة تعيين ITL من الناشر فقط. إذا قمت بإصدار إعادة تعيين ITL من مشترك، فهذا يؤدي إلى **عدم** ظهور رسالة **عقدة الناشر هذه**. يتم شرح أمثلة كل أمر بالتفصيل في الأقسام التالية.

ITLCovery باستخدام مفتاح الاسترداد المحلي

يستخدم خيار Localkey المفتاح الخاص باستعادة ITL الموجود في ملف ITLRecovery.p12 الموجود على محرك الأقراص الثابتة الخاص ب Publisher كموقع ملف ITL الجديد.

```
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
```

ITLRovery باستخدام مفتاح الاسترداد عن بعد

يسمح خيار RemoteKey لخادم SFTP الخارجي الذي تم حفظ ملف ITLRecovery.p12 منه ليتم تحديده.

```
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
```

ملاحظة: في حالة إجراء إعادة تعيين ITL باستخدام خيار RemoteKey، يتم إستبدال المفتاح المحلي (الموجود على ملف القرص) الموجود على الناشر ب RemoteKey.

التحقق من الموقع الحالي باستخدام الأمر "show itl"

إذا قمت بعرض ملف ITL باستخدام الأمر **show itl** قبل إصدار أمر إعادة تعيين ITL، فإنه يظهر أن ITL يحتوي على إدخال *<publisher_hostname>*_ITLRECOVERY. يحتوي كل ملف ITL الذي يتم تقديمه بواسطة أي خادم TFTP في نظام المجموعة على إدخال إسترداد ITL هذا من الناشر. يتم أخذ إخراج الأمر **show itl** من الناشر في هذا المثال. الرمز المميز المستخدم لتوقيع ITL غامق:

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

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

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

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

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



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

                                                                         ITL Record #:6
                                                                                  ----
                                                              BYTEPOS TAG LENGTH VALUE
                                                              ----- ------ --- -------
                                                                  RECORDLENGTH 2 713 1
                                                                       DNSNAME 2 2
    SUBJECTNAME 57 CN=test10sub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US 3
                                                                FUNCTION 2 TVS 4
     ISSUERNAME 57 CN=test10sub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US 5
```

```
SERIALNUMBER 16 67:D1:A1:9E:F8:AB:91:E6:C0:A6:10:35:26:30:EE:02 6
                                                    PUBLICKEY 270 7
                                                    SIGNATURE 256 8
CERTHASH 20 AF 28 89 16 F9 94 E6 62 A3 65 C2 88 3B 94 08 1C 66 7C 49 C9 11
                                                HASH ALGORITHM 1 SHA-1 12

.The ITL file was verified successfully
```

التحقق من إستخدام مفتاح ITLRecovery

إذا قمت بعرض ملف ITL باستخدام الأمر **show itl** بعد إجراء إعادة تعيين ITL، فإنه يظهر أن إدخال ITLRecvery قد وقع على ITL كما هو موضح هنا. ويظل ITLRecovery هو الموقع الخاص بسجل المعاملات الدولي إلى أن تتم إعادة تشغيل TFTP، وفي ذلك الوقت يتم إستخدام شهادة **callManager.pem** أو TFTP لتوقيع سجل المعاملات الدولي مرة أخرى.

```
                                                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
                                                ----- ------ --- -------
                                                        SIGNERID 2 157 3
SIGNERNAME 66 CN=ITLRECOVERY_test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US 4
                        SERIALNUMBER 16 6E:3F:65:C2:97:B3:E0:1F:E7:42:81:AB:52:CC:55:DC 5
    CANAME 66 CN=ITLRECOVERY_test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US 6
                                                    SIGNATUREINFO 2 15 7
                                                    DIGESTALGORTITHM 1 8
                                                SIGNATUREALGOINFO 2 8 9
                                                SIGNATUREALGORTITHM 1 10
                                                SIGNATUREMODULUS 1 11
                                                        SIGNATURE 128 12
                                                ff ed a ea 1b 9a c4 58
                                                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
                                                c3 f0 1d c0 e 6 1b 97
                                                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
                                                3d a3 78 dd 42 f0 af 28
                                                9d f1 42 5e 35 3c bc ae
                                                c 3 df 89 9 f9 ac 77
                                                1f 84 f5 83 d0 cc 11 60
                                                        FILENAME 12 14
                                                        TIMESTAMP 4 15
```

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

                                                                ITL Record #:2
                                                                        ----
                                                            BYTEPOS TAG LENGTH VALUE
                                                            ----- ------ --- -------
                                                               RECORDLENGTH 2 1115 1
                                                                        DNSNAME 2 2
    SUBJECTNAME 57 CN=test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US 3
                                                                FUNCTION 2 TFTP 4
     ISSUERNAME 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
                                                                PUBLICKEY 140 7
                                                                SIGNATURE 128 8
CERTIFICATE 684 01 9C 4C 3D 27 D7 4D 82 CB B1 84 84 D4 2A 63 9F 71 78 BE A9 9
                                                                (SHA1 Hash HEX)

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

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

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

```
----- ------ --- -------
                                                  RECORDLENGTH 2 1141 1
                                                       DNSNAME 2 2
SUBJECTNAME 66 CN=ITLRECOVERY_test10pub.joemar2.lab;OU=tac;O=cisco;L=rtp;ST=nc;C=US 3
                                    FUNCTION 2 System Administrator Security Token 4
 ISSUERNAME 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
                                                       PUBLICKEY 140 7
                                                       SIGNATURE 128 8
          CERTIFICATE 692 CD C7 4A 39 87 87 52 FA B0 89 0C 28 AB CB 36 32 EB 87 16 DC 9
                                                       (SHA1 Hash HEX)
                                    .This etoken was used to sign the ITL file

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

                                                .The ITL file was verified successfully
```

تحسينات لتقليل إمكانية فقدان الهواتف للثقة

بالإضافة إلى إمكانية إعادة ضبط ITL، يتضمن CUCM الإصدار 10.0(1) ميزات المسؤول التي تساعد على منع الهواتف من الدخول إلى حالة غير موثوق بها. نقطتا الثقة في الهاتف هما شهادة **TVS.PEM** (TVS) وشهادة TFTP **callManager.pem**). في ابسط بيئة مع خادم CUCM واحد فقط، إذا قام المسؤول بإعادة إنشاء شهادة **callManager.pem** وشهادة **TVS.pem** واحدة تلو الأخرى، فإنه يتم إعادة ضبط الهاتف ويعرض عند بدء التشغيل رسالة **فشل تحديث قائمة الثقة**. حتى مع إعادة تعيين الجهاز التلقائي المرسلة من CUCM إلى الهاتف بسبب شهادة موجودة في ITL يتم إعادة إنشائها، يمكن أن يدخل الهاتف حالة لا يثق فيها CUCM.

للمساعدة في منع السيناريو الذي يتم فيه إعادة إنشاء شهادات متعددة في نفس الوقت (عادة تغيير اسم المضيف أو تعديلات اسم مجال DNS)، يحتوي CUCM الآن على مؤقت إحتجاز. عند إعادة إنشاء الشهادة، يمنع CUCM المسؤول من إعادة إنشاء شهادة أخرى على نفس العقدة في غضون خمس دقائق من إعادة إنشاء الشهادة السابقة. تتسبب هذه العملية في إعادة ضبط الهواتف عند إعادة إنشاء الشهادة الأولى، ويجب أن يتم نسخها إحتياطيا وتسجيلها قبل إعادة إنشاء الشهادة التالية.

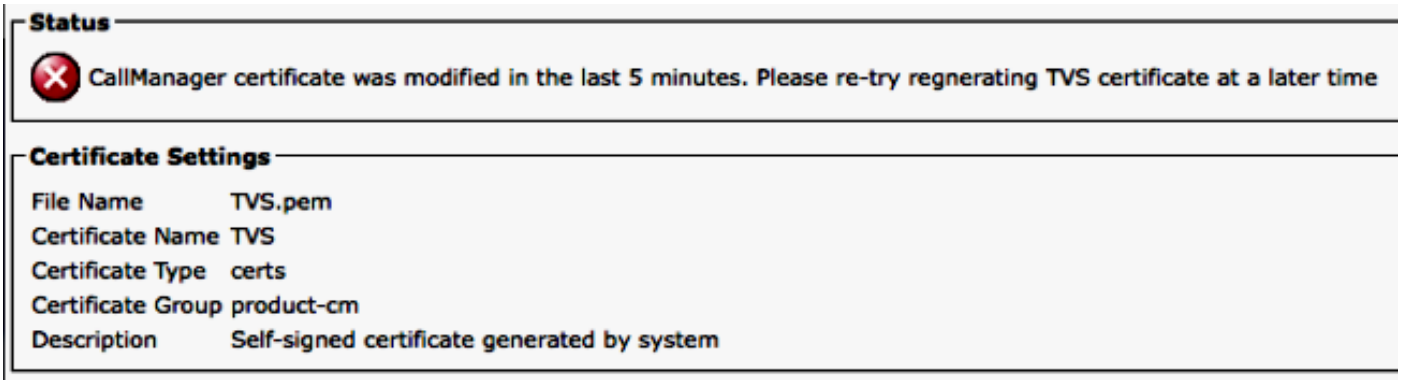
بغض النظر عن الشهادة التي يتم إنشاؤها أولا، فإن الهاتف لديه الطريقة الثانوية لمصادقة الملفات. يمكن العثور على تفاصيل إضافية حول هذه العملية في أمان "إدارة الاتصالات" بشكل افتراضي وعملية ITL واستكشاف الأخطاء واصلاحها.

يوضح هذا الإخراج حالة يمنع فيها CUCM المسؤول من إعادة إنشاء شهادة أخرى في غضون خمس دقائق من إعادة إنشاء الشهادة السابقة كما هو معروض من واجهة سطر الأوامر:

```
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
```

يمكن مشاهدة الرسالة نفسها من صفحة إدارة نظام التشغيل (OS) كما هو موضح هنا:



مفتاح الاسترداد الخاص ب ITL Publisher هو المفتاح الوحيد المستخدم بواسطة المجموعة بأكملها، على الرغم من أن كل عقدة لديها شهادة ITLRovery خاصة بها تم إصدارها للاسم الشائع (CN) الخاص ب **ITLRecovery_<*node*>**. مفتاح ITLRecovery Publisher هو المفتاح الوحيد المستخدم في ملفات ITL للمجموعة بأكملها كما هو موضح من الأمر **show itl**. ولهذا السبب يحتوي الإدخال الوحيد **ITLRecovery_<*hostname*>** الذي يظهر في ملف ITL على اسم المضيف الخاص بالناشر.

وإذا تم تغيير اسم المضيف الخاص بالناشر، يستمر إدخال ITLRecovery في ITL في إظهار اسم المضيف القديم الخاص بالناشر. ويتم القيام بذلك عن قصد لأنه لا ينبغي أبدا تغيير ملف ITLRecovery لضمان أن الهواتف تثق دائما في إسترداد ITL.

ينطبق هذا على حالة تغيير أسماء المجالات أيضا، حيث يظهر اسم المجال الأصلي في إدخال ITLRecovery لضمان عدم تغيير مفتاح الاسترداد. الوقت الوحيد الذي يجب فيه تغيير شهادة ITLRovery هو وقت انتهاء صلاحيتها لخمس سنوات ويجب إعادة إنشائها.

يمكن إعادة إنشاء أزواج المفاتيح الخاصة باسترداد ITL باستخدام واجهة سطر الأوامر (CLI) أو صفحة إدارة نظام التشغيل. لا يتم إعادة تعيين هواتف IP عند إعادة إنشاء شهادة ITLRovery على الناشر أو أي من المشتركين. بمجرد إعادة إنشاء شهادة ITLRecovery، لا يتم تحديث ملف ITL حتى تتم إعادة تشغيل خدمة TFTP. بعد إعادة إنشاء شهادة ITLRecovery على الناشر، قم بإعادة تشغيل خدمة TFTP على كل عقدة تقوم بتشغيل خدمة TFTP في نظام المجموعة لتحديث إدخال ITLRecovery في ملف ITL باستخدام الشهادة الجديدة. تتمثل الخطوة الأخيرة في إعادة ضبط جميع الأجهزة من **النظام > معلمات المؤسسة** واستخدام زر إعادة الضبط لجعل جميع الأجهزة تقوم بتنزيل ملف ITL الجديد الذي يحتوي على شهادة ITLRovery الجديدة.

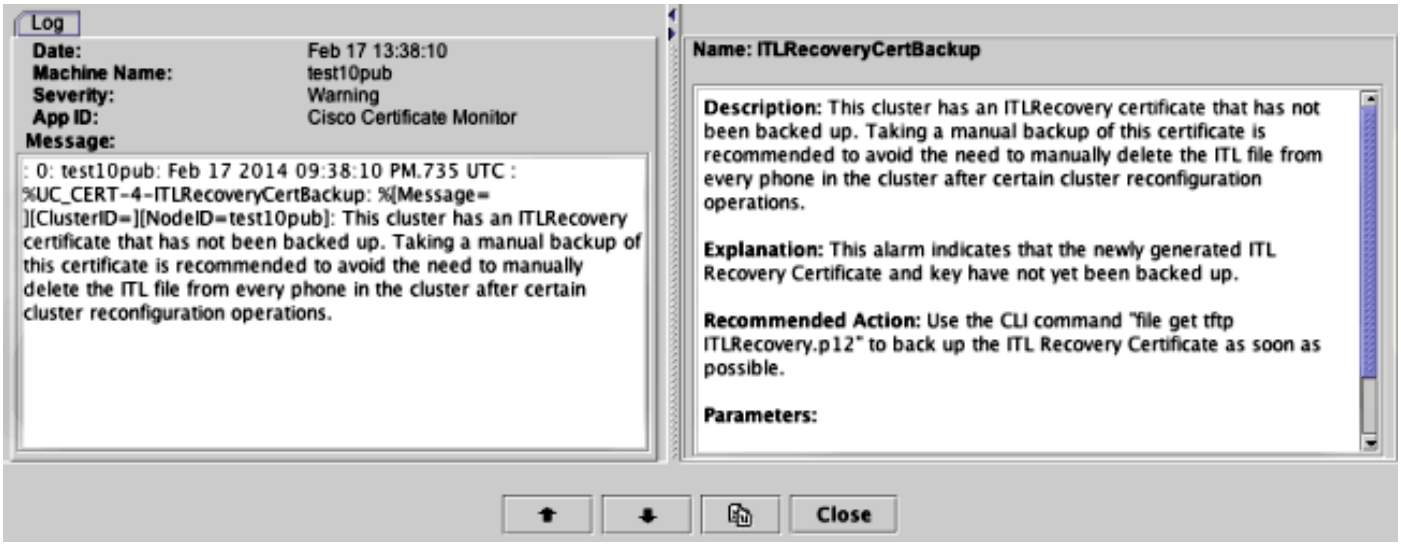
النسخ الاحتياطي لاسترداد سجل المعاملات الدولي (ITL)

يلزم توفر مفتاح إسترداد ITL لاسترداد الهواتف عند إدخالها في حالة غير موثوق بها. ونظرا لذلك، يتم إنشاء تنبيهات جديدة لأداة مراقبة الوقت الفعلي (RTMT) يوميا حتى يتم إجراء نسخ إحتياطي لمفتاح إسترداد ITL. لا يكفي النسخ الاحتياطي لنظام إسترداد البيانات بعد الكوارث (DRS) لإيقاف التنبيهات. وعلى الرغم من أنه يوصى بإجراء عملية نسخ إحتياطي لحفظ مفتاح إسترداد ITL، إلا أنه يلزم أيضا إجراء نسخ إحتياطي يدوي للملف الرئيسي.

لإجراء نسخ إحتياطي لمفتاح الاسترداد، قم بتسجيل الدخول إلى CLI الخاص بالناشر وأدخل الأمر **get tftp ITLRecovery.p12**. يلزم خادم SFTP لحفظ الملف كما هو موضح هنا. لا تحتوي عقد المشترك على ملف إسترداد ITL، لذلك إذا قمت بإصدار الأمر **get tftp ITLRecovery.p12** على مشترك، فإنه ينتج عنه **عدم العثور على الملف**.

```
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
```

إلى أن يتم إجراء النسخ الاحتياطي اليدوي من واجهة سطر الأوامر لإجراء نسخ إحتياطي لملف ITLRecovery.p12، يتم طباعة تحذير في CiscoSyslog (عارض الأحداث - سجل التطبيقات) كل يوم كما هو موضح هنا. كما يمكن أيضا تلقي بريد إلكتروني يومي حتى يتم إجراء النسخ الاحتياطي اليدوي في حالة تمكين إعلام البريد الإلكتروني من صفحة إدارة نظام التشغيل، **التأمين > مراقبة الشهادات**.



بينما تحتوي النسخ الاحتياطي ل DRS على ITLRecovery، يوصى باستمرار تخزين ملف ITLRecovery.p12 في موقع آمن في حالة فقدان ملفات النسخ الاحتياطي أو تلفها أو للحصول على خيار إعادة تعيين ملف ITL دون الحاجة إلى الاستعادة من نسخة إحتياطية. إذا كان لديك ملف ITLRecovery.p12 من الناشر المحفوظ، فإنه يسمح أيضا بإعادة إنشاء الناشر بدون نسخة إحتياطية باستخدام خيار إستعادة DRS لاستعادة قاعدة البيانات من عنصر مشاركة وإعادة إنشاء الثقة بين الهواتف وخوادم CUCM عن طريق إعادة تعيين ITL باستخدام خيار **إعادة تعيين مفتاح** التحكم عن بعد **في** UTILS.

تذكر أنه إذا تم إعادة إنشاء الناشر، يجب أن تكون كلمة مرور أمان نظام المجموعة هي نفسها الناشر الذي تم أخذ ملف ITLRecovery.p12 منه لأن ملف ITLRecovery.p12 محمي بكلمة مرور استنادا إلى كلمة مرور أمان نظام المجموعة. ولهذا السبب، إذا تم تغيير كلمة مرور أمان نظام المجموعة، فإن تنبيه RTMT الذي يشير إلى أن ملف ITLRecovery.p12 لم يتم نسخه إحتياطيا يتم إعادة تعيينه ويتم تشغيله يوميا حتى يتم حفظ ملف

ITLRecovery.p12 الجديد باستخدام الأمر **get tftp ITLRecovery.p12**.

التحقق من الصحة

لا تعمل ميزة إعادة تعيين ITL المجمع إلا إذا كانت الهواتف قد تم تثبيت ITL يحتوي على إدخال ITLRecovery. للتحقق من أن ملف ITL المثبت على الهواتف يحتوي على إدخال ITLRecovery، أدخل الأمر **show itl** من واجهة سطر الأوامر (CLI) على كل خادم من خوادم TFTP للعثور على المجموع الاختباري لملف ITL. يعرض الإنتاج من **الأمر show itl** المجموع الاختباري:

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

المجموع الاختباري مختلف على كل خادم TFTP لأن كل خادم لديه شهادة **callManager.pem** خاصة به في ملف ITL الخاص به. ويمكن العثور على المجموع الاختباري لسجل المعاملات الدولي (ITL) المثبت على الهاتف إذا قمت بعرض سجل المعاملات الدولي على الهاتف نفسه ضمن **الإعدادات > تكوين الأمان > قائمة الثقة**، من صفحة الويب الخاصة بالهاتف، أو من تنبيه DeviceTLInfo الذي تم الإعلام عنه بواسطة الهواتف التي تقوم بتشغيل البرامج الثابتة الأحدث.

تقوم معظم الهواتف التي تشغل الإصدار 9.4(1) من البرنامج الثابت أو تقوم بالإبلاغ عن تجزئة SHA1 من ITL الخاص بها إلى CUCM باستخدام تنبيه DeviceTLInfo. يمكن عرض المعلومات المرسلة بواسطة الهاتف في "عارض الأحداث" - سجل التطبيقات من RTMT ومقارنتها بتجزئة SHA1 لمخزن ITL الخاص بخوادم TFTP التي تستخدمها الهواتف للعثور على أي هواتف لم يتم تثبيت ITL الحالي عليها، والتي تحتوي على إدخال ITLRecovery.

كافيتس

- CSCun18578 - فشل إعادة ضبط ITL للمفتاح المحلي/مفتاح RemoteKey في سيناريوهات معينة
- CSCun1912 - خطأ إعادة تعيين ITL RemoteKey في نوع مصادقة SFTP غير صحيحة

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).