Unified Communications Manager ITL-Verbesserungen in Version 10.0(1)

Inhalt

[Einführung](#)
[Hintergrund](#)
[Problemsymptome](#)
[Lösung - Bulk ITL Reset](#)
[ITLR-Wiederherstellung mit dem lokalen Wiederherstellungsschlüssel](#)
[ITLR-Wiederherstellung mit dem Remote Recovery Key](#)
[Überprüfen Sie den aktuellen Signierer mit dem Befehl "show itl".](#)
[Überprüfen Sie, ob der ITLR-Wiederherstellungsschlüssel verwendet wird.](#)
[Verbesserungen zur Reduzierung der Wahrscheinlichkeit, dass Telefone das Vertrauen verlieren](#)
[Sichern der ITL-Wiederherstellung](#)
[Überprüfen](#)
[Einsprüche](#)

Einführung

Dieses Dokument beschreibt eine neue Funktion in Cisco Unified Communications Manager (CUCM) Version 10.0(1), die das Zurücksetzen von ITL-Dateien (Identity Trust List) auf Cisco Unified IP-Telefonen ermöglicht. Die Funktion zum Zurücksetzen von Massensets für ITL wird verwendet, wenn Telefone nicht mehr dem ITL-Dateisigner vertrauen und die vom TFTP-Dienst lokal oder mithilfe des TVS (Trust Verification Service) bereitgestellte ITL-Datei nicht authentifizieren können.

Hintergrund

Da ITL-Dateien mehrmals zurückgesetzt werden können, müssen mindestens ein dieser Schritte ausgeführt werden, um die Vertrauenswürdigkeit zwischen IP-Telefonen und den CUCM-Servern wiederherzustellen.

- Wiederherstellen von einer Sicherung, um eine alte ITL-Datei hochzuladen, der die Telefone vertrauen
- Ändern Sie die Telefone, um einen anderen TFTP-Server zu verwenden.
- Löschen Sie die ITL-Datei über das Einstellungsmenü manuell vom Telefon.
- Zurücksetzen des Telefons in den Ereigniseinstellungen, sodass der Zugriff deaktiviert ist, um die ITL zu löschen

Diese Funktion soll Telefone nicht zwischen Clustern verschieben. Verwenden Sie für diese

Aufgabe eine der Methoden, die unter Migration von IP-Telefonen zwischen Clustern mit CUCM 8- und ITL-Dateien beschrieben ist. Der ITL-Reset-Vorgang wird nur verwendet, um die Vertrauenswürdigkeit zwischen IP-Telefonen und dem CUCM-Cluster wiederherzustellen, wenn diese ihre Vertrauenspunkte verloren haben.

Eine weitere in CUCM Version 10.0(1) verfügbare sicherheitsrelevante Funktion, die in diesem Dokument nicht behandelt wird, ist die CTL (Tokenless Certificate Trust List). Die Tokenless CTL ersetzt die Hardware-USB-Sicherheitstoken durch ein Software-Token, das zur Aktivierung der Verschlüsselung auf den CUCM-Servern und -Endpunkten verwendet wird. Weitere Informationen finden Sie im Dokument IP Phone Security and CTL (Certificate Trust List).

Weitere Informationen zu den ITL-Dateien und standardmäßig zur Sicherheit finden Sie im Dokument Communications Manager Security By Default und ITL Operation and Troubleshooting (Communications Manager-Standardsicherheit).

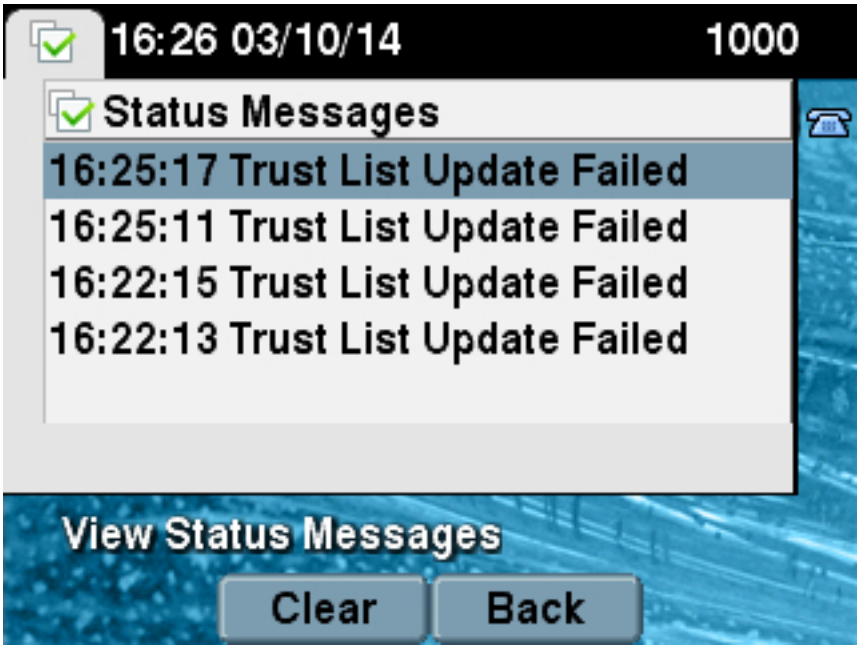
Problemsymptome

Wenn sich die Telefone in einem **gesperrten** oder **nicht vertrauenswürdigen** Zustand befinden, akzeptieren sie die vom TFTP-Dienst bereitgestellte ITL-Datei- oder TFTP-Konfiguration nicht. Konfigurationsänderungen, die in der TFTP-Konfigurationsdatei enthalten sind, werden nicht auf das Telefon angewendet. Einige Beispiele für Einstellungen, die in der TFTP-Konfigurationsdatei enthalten sind, sind:

- Zugriff auf Einstellungen
- Webzugriff
- Secure Shell (SSH)-Zugriff
- Switched Port Analyzer (SPAN) an PC-Port

Wenn eine dieser Einstellungen für ein Telefon auf der CCM-Administratorseite geändert wird und die Änderungen nach dem Zurücksetzen des Telefons nicht wirksam werden, wird dem TFTP-Server möglicherweise nicht vertraut. Ein weiteres häufiges Symptom ist, wenn Sie auf das Firmenverzeichnis oder andere Telefondienste zugreifen, die Meldung **Host Not Found** (Host nicht gefunden) wird angezeigt. Um zu überprüfen, ob sich das Telefon in einem gesperrten oder nicht vertrauenswürdigen Zustand befindet, überprüfen Sie die Telefonstatusmeldungen vom Telefon selbst oder von der Telefon-Webseite, um zu sehen, ob eine Meldung **Vertrauenslistenaktualisierung fehlgeschlagen** angezeigt wird. Die Meldung **"ITL Update Failed"** (ITL-Aktualisierung fehlgeschlagen) gibt an, dass sich das Telefon in einem gesperrten oder nicht vertrauenswürdigen Zustand befindet, da es die Vertrauensliste mit dem aktuellen ITL nicht authentifiziert und nicht mit TVS authentifiziert hat.

Die Meldung **Vertrauenswürdiger Listenupdate Failed** (Aktualisierung der Vertrauensliste fehlgeschlagen) wird vom Telefon angezeigt, wenn Sie zu **Einstellungen > Status > Status Messages (Einstellungen > Statusmeldungen)** navigieren:



Die Meldung **Vertrauenslistenaktualisierungen fehlgeschlagen** kann auch auf der Telefon-Webseite in den **Statusmeldungen** angezeigt werden, wie hier gezeigt:

Lösung - Bulk ITL Reset

CUCM-Version 10.0(1) verwendet einen zusätzlichen Schlüssel, der verwendet werden kann, um die Vertrauenswürdigkeit zwischen Telefonen und den CUCM-Servern wiederherzustellen. Dieser neue Schlüssel ist der ITL-Wiederherstellungs-Schlüssel. Der ITL Recovery Key wird während der Installation oder Aktualisierung erstellt. Dieser Wiederherstellungsschlüssel ändert sich nicht, wenn Hostnamenänderungen, DNS-Änderungen oder andere Änderungen durchgeführt werden, die zu Problemen führen können, bei denen die Telefone in einen Zustand gelangen, in dem sie dem Signator ihrer Konfigurationsdateien nicht mehr vertrauen.

Der Befehl **utils itl reset** CLI kann verwendet werden, um die Vertrauenswürdigkeit zwischen einem Telefon oder Telefonen und dem TFTP-Dienst auf dem CUCM wiederherzustellen, wenn sich Telefone in einem Zustand befinden, in dem die Meldung **Trust List Update Failed (Aktualisierung der Liste fehlgeschlagen)** angezeigt wird. Befehl **utils itl reset**:

1. Wechselt die aktuelle ITL-Datei vom Herausgeberknoten, entfernt die Signatur der ITL-Datei und signiert den Inhalt der ITL-Datei erneut mit dem privaten ITL Recovery-Schlüssel.
2. Kopiert die neue ITL-Datei automatisch in die TFTP-Verzeichnisse aller aktiven TFTP-Knoten im Cluster.
3. Startet die TFTP-Services automatisch auf jedem Knoten neu, auf dem TFTP ausgeführt

wird.

Der Administrator muss dann alle Telefone zurücksetzen. Das Zurücksetzen veranlasst die Telefone, die ITL-Datei beim Hochfahren vom TFTP-Server anzufordern, und die ITL-Datei, die das Telefon empfängt, wird statt des privaten Schlüssels **callmanager.pem** vom ITLRecovery-Schlüssel signiert. Es gibt zwei Optionen zum Ausführen einer ITL-Zurücksetzung: **utils itl reset localkey** und **utils itl reset remotekey**. Der ITL-Rücksetzbefehl kann nur vom Publisher ausgeführt werden. Wenn Sie ein ITL-Zurücksetzen von einem Teilnehmer vornehmen, wird die Meldung **This is not a Publisher Node (Dies ist kein Herausgeber-Knoten) angezeigt**. Beispiele für die einzelnen Befehle finden Sie in den folgenden Abschnitten.

ITLR-Wiederherstellung mit dem lokalen Wiederherstellungsschlüssel

Die localkey-Option verwendet den privaten ITL Recovery-Schlüssel, der in der auf der Publisher-Festplatte vorhandenen Datei ITLRecovery.p12 enthalten ist, als neuen ITL-Dateisigner.

```
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
```

ITLR-Wiederherstellung mit dem Remote Recovery Key

Mit der Remote-Schlüsseloption kann der externe SFTP-Server, von dem aus die Datei ITLRecovery.p12 gespeichert wurde, angegeben werden.

```
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
```

Hinweis: Wenn eine ITL-Rücksetzung mit der Remote-Schlüsseloption erfolgt, wird der localkey (auf der Datenträgerdatei) auf dem Herausgeber durch den Remote-Schlüssel ersetzt.

Überprüfen Sie den aktuellen Signierer mit dem Befehl "show itl".

Wenn Sie die ITL-Datei mit dem Befehl **show itl** anzeigen, bevor Sie einen ITL-Reset-Befehl ausgeben, zeigt dies, dass die ITL einen **ITLRECOVERY_*<publisher_hostname>*** Eintrag enthält. Jede ITL-Datei, die von einem TFTP-Server im Cluster bereitgestellt wird, enthält diesen ITL-Wiederherstellungs-Eintrag vom Publisher. Die Ausgabe des Befehls **show itl** wird vom Herausgeber in diesem Beispiel übernommen. Das Token zum Signieren der ITL ist fett formatiert:

```
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.
```

Überprüfen Sie, ob der ITLR-Wiederherstellungsschlüssel verwendet wird.

Wenn Sie die ITL-Datei mit dem Befehl **show itl** anzeigen, nachdem Sie einen ITL-Reset durchgeführt haben, zeigt dies, dass der ITLRecovery-Eintrag das ITL signiert hat, wie hier gezeigt. Die ITLR-Wiederherstellung bleibt bis zum Neustart des TFTP der Signatur des ITL. Anschließend wird das **callmanager.pem-** oder TFTP-Zertifikat verwendet, um das ITL erneut zu signieren.

```
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.
```

Verbesserungen zur Reduzierung der Wahrscheinlichkeit, dass Telefone das Vertrauen verlieren

Zusätzlich zur ITL-Rücksetzfunktion enthält die CUCM-Version 10.0(1) Administratorfunktionen, die verhindern, dass Telefone in einen nicht vertrauenswürdigen Zustand wechseln. Die beiden Vertrauenspunkte, über die das Telefon verfügt, sind das TVS-Zertifikat (**TVS.pem**) und das TFTP-Zertifikat (**callmanager.pem**). Wenn ein Administrator in der einfachsten Umgebung mit nur einem CUCM-Server das **callmanager.pem-**Zertifikat und das **TVS.pem-**Zertifikat direkt nach dem anderen neu generiert, setzt das Telefon das Telefon zurück und zeigt beim Starten die Meldung **Trust List Update Failed (Aktualisierung der Vertrauensliste fehlgeschlagen)** an. Selbst bei einem automatischen Zurücksetzen des Geräts, das vom CUCM an das Telefon gesendet wird, aufgrund eines Zertifikats in der ITL, das neu generiert wird, kann das Telefon in einen Zustand wechseln, in dem es CUCM nicht vertraut.

Um zu verhindern, dass mehrere Zertifikate gleichzeitig neu generiert werden (in der Regel Änderung des Hostnamens oder des DNS-Domänennamen), verfügt der CUCM jetzt über einen Hold-Timer. Wenn ein Zertifikat neu generiert wird, verhindert CUCM, dass der Administrator innerhalb von fünf Minuten nach der vorherigen Zertifikatwiederherstellung ein weiteres Zertifikat auf demselben Knoten neu generiert. Bei diesem Vorgang werden die Telefone nach der Wiederherstellung des ersten Zertifikats zurückgesetzt. Sie sollten gesichert und registriert werden, bevor das nächste Zertifikat neu generiert wird.

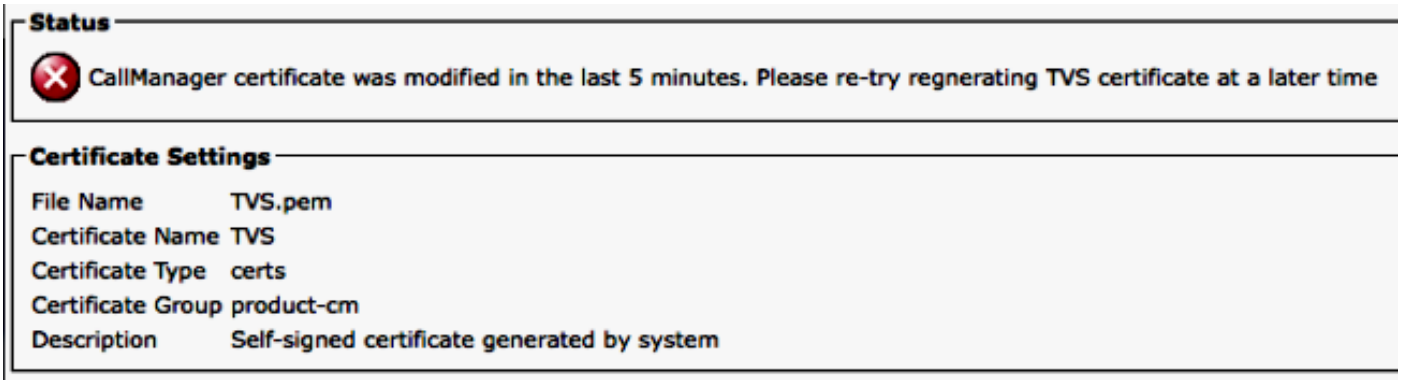
Unabhängig davon, welches Zertifikat zuerst generiert wird, verfügt das Telefon über eine sekundäre Methode zum Authentifizieren von Dateien. Weitere Einzelheiten zu diesem Prozess finden Sie unter Communications Manager Security By Default und ITL Operation and Troubleshooting.

Diese Ausgabe zeigt eine Situation, in der CUCM den Administrator daran hindert, innerhalb von fünf Minuten nach einer vorherigen Zertifikatswiederherstellung, wie in der CLI dargestellt, ein weiteres Zertifikat erneut zu erstellen:

```
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
```

Die gleiche Meldung wird auf der Seite für die Betriebssystemverwaltung angezeigt, wie hier

gezeigt:



Der Herausgeber-ITL-Wiederherstellungsschlüssel ist der einzige, der vom gesamten Cluster verwendet wird, obwohl jeder Knoten über ein eigenes ITLR-Wiederherstellungszertifikat verfügt, das dem Common Name (CN) von **ITLRecovery_*<Node name>*** ausgestellt wurde. Der ITLRecovery-Schlüssel des Herausgebers ist der einzige Schlüssel, der in den ITL-Dateien für den gesamten Cluster verwendet wird, wie im Befehl **show itl** zu sehen ist. Aus diesem Grund enthält der einzige **ITLRecovery_*<hostname>***-Eintrag in einer ITL-Datei den Hostnamen des Herausgebers.

Wenn der Hostname des Herausgebers geändert wird, zeigt der ITLRecovery-Eintrag in der ITL weiterhin den alten Hostnamen des Herausgebers an. Dies geschieht absichtlich, da sich die ITLR-Wiederherstellungsdatei nie ändern sollte, um sicherzustellen, dass die Telefone der ITL-Wiederherstellung immer vertrauen.

Dies gilt für die Änderung von Domänennamen. Der ursprüngliche Domänenname wird im ITLRecovery-Eintrag angezeigt, um sicherzustellen, dass sich der Wiederherstellungsschlüssel nicht ändert. Das ITLR-Wiederherstellungszertifikat sollte nur dann geändert werden, wenn es aufgrund der fünfjährigen Gültigkeit abläuft und neu generiert werden muss.

Die Tastenfelder für die ITL-Wiederherstellung können entweder über die CLI oder die Seite für die Betriebssystemverwaltung neu generiert werden. IP-Telefone werden nicht zurückgesetzt, wenn das ITLR-Wiederherstellungszertifikat auf dem Herausgeber oder einem der Abonnenten neu erstellt wird. Nachdem das ITLR-Wiederherstellungszertifikat neu generiert wurde, wird die ITL-Datei erst aktualisiert, wenn der TFTP-Dienst neu gestartet wurde. Nach der Erneuerung des ITLR-Zertifikats auf dem Publisher starten Sie den TFTP-Dienst auf jedem Knoten, der den TFTP-Dienst im Cluster ausführt, neu, um den ITLR-Wiederherstellungs-Eintrag in der ITL-Datei mit dem neuen Zertifikat zu aktualisieren. Der letzte Schritt besteht darin, alle Geräte von **System > Enterprise Parameters** zurückzusetzen und die Reset-Taste zu verwenden, damit alle Geräte die neue ITL-Datei herunterladen können, die das neue ITLR-Wiederherstellungszertifikat enthält.

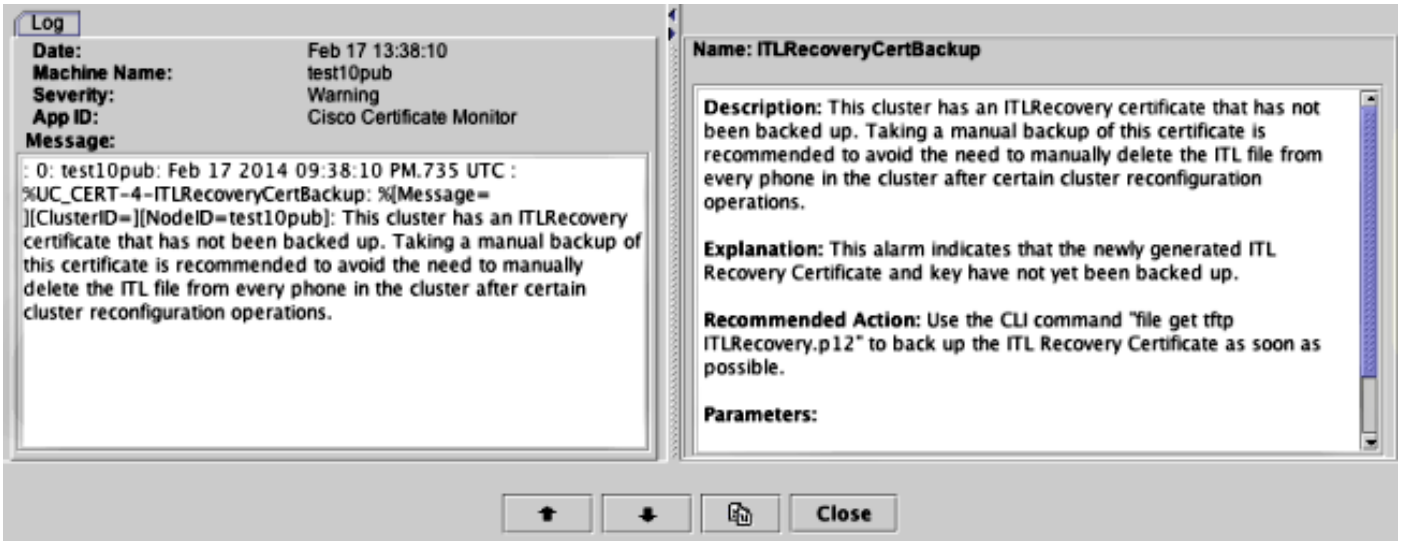
Sichern der ITL-Wiederherstellung

Der ITL-Wiederherstellungsschlüssel ist erforderlich, um Telefone wiederherzustellen, wenn sie in einen nicht vertrauenswürdigen Zustand wechseln. Aus diesem Grund werden täglich neue RTMT-Warnungen (Real-Time Monitoring Tool) generiert, bis der ITL-Wiederherstellungsschlüssel gesichert ist. Eine DRS-Sicherung (Disaster Recovery System) reicht nicht aus, um die Warnungen zu stoppen. Obwohl eine Sicherung empfohlen wird, um den ITL-Wiederherstellungsschlüssel zu speichern, ist auch eine manuelle Sicherung der Schlüsseldatei erforderlich.

Um den Wiederherstellungsschlüssel zu sichern, melden Sie sich bei der CLI des Publishers an, und geben Sie die **Datei get tftp ITLRecovery.p12**-Befehl ein. Ein SFTP-Server wird benötigt, um die Datei wie hier gezeigt zu speichern. Subscriber-Knoten verfügen nicht über eine ITL-Wiederherstellungsdatei. Wenn Sie also die **Datei "get tftp ITLRecovery.p12"** auf einem Subscriber-Befehl ausgeben, wird die **Datei nicht gefunden**.

```
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
```

Bis die manuelle Sicherung von der CLI aus durchgeführt wird, um die Datei ITLRecovery.p12 zu sichern, wird täglich eine Warnung in CiscoSyslog (Ereignisanzeige - Anwendungsprotokoll) ausgegeben, wie hier gezeigt. Eine tägliche E-Mail-Nachricht kann auch bis zur manuellen Sicherung empfangen werden, wenn die E-Mail-Benachrichtigung auf der Seite für die Betriebssystemverwaltung, **Sicherheit > Zertifikatmonitor,** aktiviert ist.



Während eine DRS-Sicherung die ITLRecovery enthält, wird empfohlen, die Datei ITLRecovery.p12 an einem sicheren Speicherort zu speichern, falls die Sicherungsdateien verloren gehen oder beschädigt sind oder um die Möglichkeit zum Zurücksetzen der ITL-Datei zu haben, ohne dass eine Sicherung wiederhergestellt werden muss. Wenn Sie die ITLRecovery.p12-Datei vom Publisher gespeichert haben, kann der Publisher auch ohne Sicherung neu erstellt werden. Hierzu wird die DRS-Wiederherstellungsoption verwendet, um die Datenbank von einem Subscriber wiederherzustellen und die Vertrauenswürdigkeit zwischen Telefonen und CUCM-Servern wiederherzustellen, indem die ITL mit der **Option** ITL **zum**

Zurücksetzen des Remote-Schlüssels zurückgesetzt wird.

Denken Sie daran, dass bei der Neuerstellung des Publishers das Sicherheitskennwort des Clusters mit dem Herausgeber identisch sein muss, von dem die Datei ITLRecovery.p12 entfernt wurde, da die Datei ITLRecovery.p12 kennwortgeschützt ist und das Kennwort auf dem Sicherheitskennwort des Clusters basiert. Aus diesem Grund wird, wenn das Sicherheitskennwort des Clusters geändert wird, die RTMT-Warnung, die anzeigt, dass die Datei ITLRecovery.p12 nicht gesichert wurde, zurückgesetzt und löst täglich aus, bis die neue Datei ITLRecovery.p12 mit dem Befehl **get tftp ITLRecovery.p12** gespeichert wird.

Überprüfen

Die Funktion zum Zurücksetzen von Massensätzen für ITLs funktioniert nur, wenn auf den Telefonen eine ITL installiert ist, die den ITLRecovery-Eintrag enthält. Um zu überprüfen, ob die auf den Telefonen installierte ITL-Datei den ITLR-Wiederherstellungs-Eintrag enthält, geben Sie den Befehl **show itl** aus der CLI auf jedem TFTP-Server ein, um die Prüfsumme der ITL-Datei zu finden. Die Ausgabe des Befehls **show itl** zeigt die Prüfsumme an:

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

Die Prüfsumme ist auf jedem TFTP-Server unterschiedlich, da jeder Server ein eigenes **callmanager.pem-**Zertifikat in seiner ITL-Datei hat. Die ITL-Prüfsumme der auf dem Telefon installierten ITL finden Sie, wenn Sie die ITL auf dem Telefon selbst unter **Einstellungen > Sicherheitskonfiguration > Vertrauensliste** anzeigen, auf der Telefon-Webseite oder im DeviceTLInfo-Alarm, der von Telefonen gemeldet wird, die neuere Firmware ausführen.

Die meisten Telefone, auf denen die Firmware Version 9.4(1) oder höher ausgeführt wird, melden den SHA1-Hash ihrer ITL mit dem DeviceTLInfo-Alarm an CUCM. Die vom Telefon gesendeten Informationen können im Event Viewer - Application Log from RTMT (Ereignisanzeige - Anwendungsprotokoll von RTMT) angezeigt und mit dem SHA1-Hash des ITL-Hashs der TFTP-Server verglichen werden, mit dem die Telefone Telefone finden, auf denen nicht die aktuelle ITL installiert ist, die den ITLRerkleinereintrag enthält.

Einsprüche

- CSCun18578 - ITL-Reset-Localkey/Remote-Key schlägt in bestimmten Szenarien fehl
- CSCun19112 - Remote-Fehler beim Zurücksetzen von ITL im SFTP-Authentifizierungstyp