버전 10.0(1)의 Unified Communications Manager ITL 개선 사항

목차

소개

이 문서에서는 Cisco Unified IP Phone에서 ITL(Identity Trust List) 파일을 대량 재설정할 수 있는 Cisco CUCM(Unified Communications Manager) 버전 10.0(1)의 새로운 기능에 대해 설명합니다 .대량 ITL 재설정 기능은 전화기가 더 이상 ITL 파일 서명자를 신뢰하지 않으며, TFTP 서비스가 로컬로 또는 TVS(Trust Verification Service)를 사용하여 제공하는 ITL 파일을 인증할 수 없는 경우에 사용됩니다.

배경

ITL 파일을 대량 재설정할 수 있으므로 IP 전화와 CUCM 서버 간의 신뢰를 다시 설정하기 위해 이러한 단계 중 하나 또는 여러 단계를 수행할 필요가 없습니다.

- 전화기에서 신뢰할 수 있는 이전 ITL 파일을 업로드하려면 백업에서 복원
- 다른 TFTP 서버를 사용하려면 전화기를 변경합니다.
- 설정 메뉴를 통해 전화기에서 ITL 파일을 수동으로 삭제합니다.
- ITL을 지우기 위해 액세스가 비활성화되도록 이벤트 설정에서 전화기를 출하 시 재설정합니다.

이 기능은 클러스터 간에 전화기를 이동시키기 위한 것이 아닙니다.이 작업의 경우 Migrating IP Phones Between Clusters with CUCM 8 and ITL Files에 설명된 방법 중 하나를 사용합니다.ITL 재설정 작업은 신뢰 지점이 손실된 경우 IP 전화와 CUCM 클러스터 간의 신뢰를 다시 설정하는 데만 사용됩니다.

CUCM 버전 10.0(1)에서 사용할 수 있는 다른 보안 관련 기능은 이 문서에서 다루지 않는

CTL(Tokenless Certificate Trust List)입니다. Tokenless CTL은 하드웨어 USB 보안 토큰을 CUCM 서버 및 엔드포인트에서 암호화를 활성화하는 데 사용되는 소프트웨어 토큰으로 교체합니다.자세한 내용은 IP Phone Security and CTL (Certificate Trust List) 문서를 참조하십시오.

ITL 파일 및 보안에 대한 추가 정보는 기본적으로 Communications Manager Security By Default(Communications Manager 보안 기준) 및 ITL Operation and Troubleshooting(ITL 작업 및 문제 해결) 문서에서 찾을 수 있습니다.

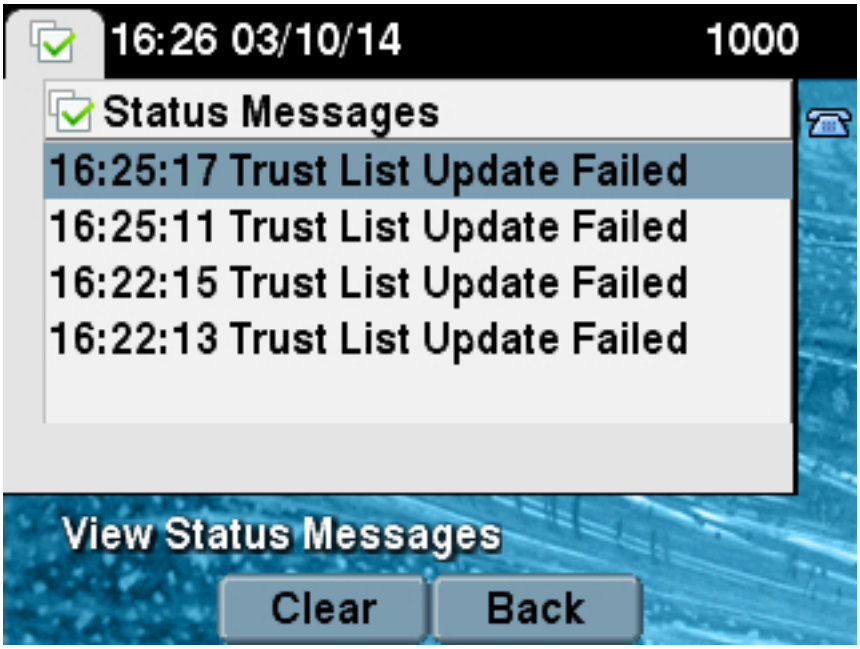
문제 증상

전화기가 **잠기거나 신뢰할 수 없는** 상태이면 TFTP 서비스에서 제공하는 ITL 파일 또는 TFTP 구성을 수락하지 않습니다.TFTP 컨피그레이션 파일에 포함된 컨피그레이션 변경 사항은 전화기에 적용되지 않습니다.TFTP 컨피그레이션 파일에 포함된 설정의 몇 가지 예는 다음과 같습니다.

- 설정 액세스
- 웹 액세스
- SSH(Secure Shell) 액세스
- SPAN(Switched Port Analyzer)에서 PC 포트로

CCM Admin(CCM 관리) 페이지에서 전화기에 대해 이러한 설정이 변경되고 전화기가 재설정된 후 변경 사항이 적용되지 않을 경우 전화기에서 TFTP 서버를 신뢰하지 않을 수 있습니다.또 다른 일반적인 증상은 회사 디렉터리 또는 다른 전화 서비스에 액세스할 때 **Host Not Found**(호스트 **없음)라는** 메시지가 표시됩니다.전화기가 잠기거나 신뢰할 수 없는 상태인지 확인하려면 전화기 자체 또는 전화 웹 페이지에서 전화 상태 메시지를 확인하여 **Trust List Update Failed** 메시지가 표시되는지 확인합니다.ITL **Update Failed(ITL 업데이트 실패**) 메시지는 전화기가 현재 ITL로 신뢰 목록을 인증하지 못하고 TVS로 인증하지 못했기 때문에 잠겨 있거나 신뢰할 수 없는 상태임을 나타내는 표시기입니다.

Settings(**설정**) > Status(상태) **> Status Messages(상태 메시지)**로 이동하면 전화기 자체에서 Trust List Update Failed(신뢰 목록 업데이트 실패) 메시지를 볼 수 있습니다.



Trust **List Update Failed** 메시지는 다음과 같이 Status Messages(**상태 메시지)**의 전화 웹 페이지에서도 볼 수 있습니다.

솔루션 - 벌크 ITL 재설정

CUCM 버전 10.0(1)은 전화기와 CUCM 서버 간의 신뢰를 다시 설정하기 위해 사용할 수 있는 추가 키를 사용합니다.이 새 키는 ITL 복구 키입니다.ITL 복구 키는 설치 또는 업그레이드 중에 생성됩니다.이 복구 키는 호스트 이름 변경, DNS 변경 또는 기타 변경 사항을 수행해도 변경되지 않으며, 이로 인해 전화기가 구성 파일의 서명자를 더 이상 신뢰하지 않는 상태가 될 수 있습니다.

새 utils **itl reset** CLI 명령은 전화기가 **Trust List Update Failed** 메시지가 표시되는 상태에 있을 때 전화나 전화와 CUCM의 TFTP 서비스 간 신뢰를 재설정하기 위해 사용할 수 있습니다.utils **itl reset** 명령:

1. 게시자 노드에서 현재 ITL 파일을 가져와 ITL 파일의 서명을 제거하고 ITL 복구 개인 키를 사용하여 ITL 파일의 내용을 다시 서명합니다.
2. 새 ITL 파일을 클러스터에 있는 모든 활성 TFTP 노드의 TFTP 디렉토리에 자동으로 복사합니다.
3. TFTP가 실행되는 모든 노드에서 TFTP 서비스를 자동으로 재시작합니다.

그런 다음 관리자가 모든 전화기를 재설정해야 합니다.재설정은 TFTP 서버에서 부팅할 때 전화기에서 ITL 파일을 요청하도록 하며, 전화기에서 수신하는 ITL 파일은 callmanager.pem 개인 키 대신 ITLRecovery 키**에서 서명됩니다**.ITL 재설정을 실행하는 두 가지 옵션이 있습니다.**utils itl reset localkey** 및 utils **itl reset remotekey**.ITL 재설정 명령은 게시자에서만 실행할 수 있습니다.가입자에서 ITL 재설정을 실행하면 **This is not a Publisher Node** 메시지**가** 표시됩니다.각 명령의 예는 다음 섹션에서 자세히 설명합니다.

ITLR로컬 복구 키를 사용한 복구

localkey 옵션은 Publisher 하드 드라이브에 있는 ITLRecovery.p12 파일에 포함된 ITL 복구 개인 키를 새 ITL 파일 서명자로 사용합니다.

```
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
```

원격 복구 키를 사용한 ITLRecovery

remotekey 옵션을 사용하면 ITLRecovery.p12 파일이 저장된 외부 SFTP 서버를 지정할 수 있습니다.

```
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
```

> **참고:**remotekey 옵션을 사용하여 ITL 재설정을 수행하면 게시자의 localkey(디스크 파일의 localkey)가 remotekey로 바뀝니다.

"show itl" 명령으로 현재 서명자 확인

ITL reset 명령을 실행하기 전에 show itl 명령으로 ITL 파일을 볼 경우 ITL에 ITLRECOVERY_*<publisher_hostname>* 항목이 포함되어 있음을 표시합니다.클러스터의 모든 TFTP 서버에서 제공하는 모든 ITL 파일에는 게시자의 이 ITL 복구 항목이 포함되어 있습니다.이 예에서 **show** itl 명령의 출력은 게시자에서 가져옵니다.ITL에 서명하기 위해 사용되는 토큰은 굵게 표시됩니다.

```
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 키가 사용되는지 확인합니다.

ITL 재설정을 수행한 후 **show itl** 명령으로 ITL 파일을 보면 ITLRecovery 항목이 여기에 표시된 대로 ITL에 서명했음을 알 수 있습니다.ITLRecovery는 TFTP가 재시작될 때까지 ITL의 서명자(ITL에 다시 서명하기 위해 callmanager.**pem** 또는 TFTP 인증서가 사용됨)로 유지됩니다.

```
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.
```

전화 신뢰 손실 가능성을 줄이기 위한 개선 사항

ITL 재설정 기능 외에도 CUCM 버전 10.0(1)에는 전화기가 신뢰할 수 없는 상태로 들어가는 것을 방지하는 관리자 기능이 포함되어 있습니다.전화기에 있는 두 신뢰 지점은 TVS 인증서(**TVS.pem**)와 TFTP 인증서(callmanager.**pem**)입니다. 단 하나의 CUCM 서버만 있는 가장 단순한 환경에서 관리자가 callmanager.pem 인증서 및 TVS.**pem** 인증서를 차례로 재생성하는 경우 전화기가 재설정되고 부팅 시 **Trust List Update Failed** 메시지가 표시됩니다.재생성된 ITL에 포함된 인증서로 인해 CUCM에서 전화로 자동 디바이스 재설정이 전송되더라도 전화기는 CUCM을 신뢰하지 않는 상태로 들어갈 수 있습니다.

여러 인증서가 동시에 재생성되는 상황을 방지하기 위해(일반적으로 호스트 이름 변경 또는 DNS 도메인 이름 수정) CUCM에는 보류 타이머가 있습니다.인증서가 재생성되면 CUCM은 관리자가 이전 인증서 재생성 후 5분 이내에 동일한 노드에 있는 다른 인증서를 재생성하지 못하도록 합니다.이 프로세스를 수행하면 첫 번째 인증서를 재생성할 때 전화기가 재설정되며, 다음 인증서를 다시 생성하기 전에 전화기를 백업하고 등록해야 합니다.

어떤 인증서가 먼저 생성되었는지에 관계없이 전화기에 파일을 인증하는 보조 방법이 있습니다.이 프로세스에 대한 자세한 내용은 Communications Manager Security By Default(기본) 및 ITL Operation and Troubleshooting(ITL 작업 및 문제 해결)에서 확인할 수 있습니다.

이 출력은 CUCM이 CLI에서 볼 수 있듯이 이전 인증서 재생성 후 5분 내에 관리자가 다른 인증서를 재생성하지 못하도록 하는 상황을 보여줍니다.

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

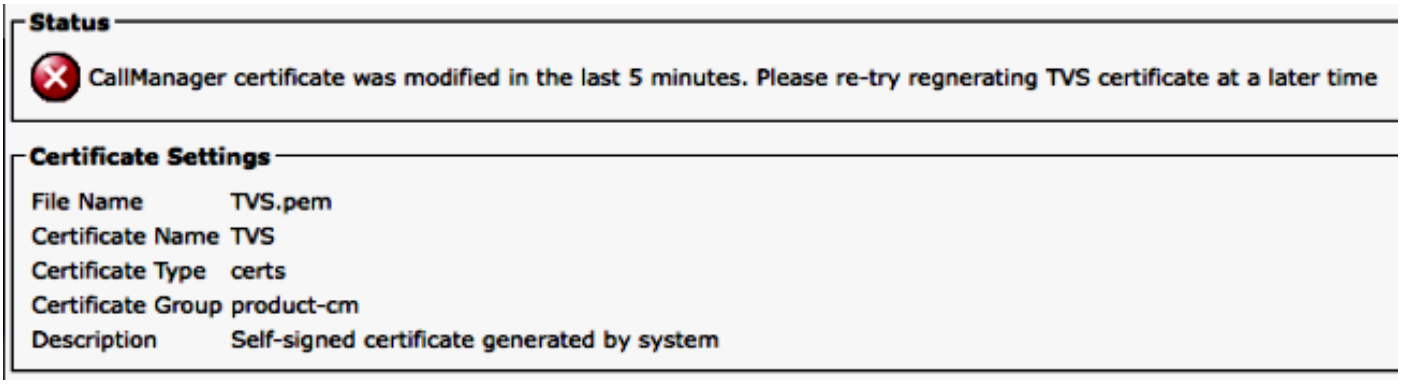
```
WARNING: This operation will overwrite any CA signed certificate
previously imported for CallManager
Proceed with regeneration (yes|no)? yes


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
```

다음과 같이 OS(운영 체제) 관리 페이지에서 동일한 메시지를 볼 수 있습니다.



게시자 ITL 복구 키는 ITLRecovery_*<node name>*의 CN(Common Name)에 발급된 고유 ITLRecovery 인증서가 각 노드에 있더라도 전체 클러스터**에서** 사용 중인 유일한 ***키입니다***.게시자 ITLRecovery 키는 show itl 명령에서 볼 수 있는 것처럼 전체 클러스터의 ITL 파일에 사용되는 유일한 **키입니다**.따라서 ITL 파일에 표시된 유일한 **ITLRecovery_*<hostname>*** 항목에 게시자의 호스트 이름이 포함됩니다.

게시자의 호스트 이름이 변경되면 ITL의 ITLRecovery 항목이 게시자의 이전 호스트 이름을 계속 표시합니다.이는 ITLRecovery 파일이 변경되지 않아야 전화기가 ITL 복구를 항상 신뢰하도록 하기 때문에 의도적으로 수행됩니다.

도메인 이름이 변경될 때도 적용됩니다.복구 키가 변경되지 않도록 하기 위해 원래 도메인 이름이 ITLRecovery 항목에 표시됩니다.ITLRecovery 인증서가 5년 유효성으로 만료되어 다시 생성되어야 하는 경우에만 ITLRecovery 인증서가 변경됩니다.

ITL 복구 키 쌍은 CLI 또는 OS Administration(OS 관리) 페이지에서 다시 생성할 수 있습니다 .ITLRecovery 인증서가 게시자 또는 구독자에서 다시 생성될 때 IP 전화가 재설정되지 않습니다 .ITLRecovery 인증서가 재생성되면 TFTP 서비스가 재시작될 때까지 ITL 파일이 업데이트되지 않습니다.게시자에서 ITLRecovery 인증서 재생성 후 ITL 파일의 ITLRecovery 항목을 새 인증서로 업데이트하려면 클러스터에서 TFTP 서비스를 실행하는 모든 노드에서 TFTP 서비스를 다시 시작합니다.마지막 단계는 **System(시스템) > Enterprise Parameters(엔터프라이즈 매개변수)**에서 모든 디바이스를 재설정하고 재설정 버튼을 사용하여 모든 디바이스에서 새 ITLRecovery 인증서가 포함된 새 ITL 파일을 다운로드하도록 하는 것입니다.

ITL 복구 백업

신뢰할 수 없는 상태가 되면 전화기를 복구하려면 ITL 복구 키가 필요합니다.이 때문에 ITL

Recovery 키가 백업될 때까지 새로운 RTMT(Real-Time Monitoring Tool) 알림이 매일 생성됩니다 .DRS(Disaster Recovery System) 백업으로는 경고를 중지할 수 없습니다.ITL 복구 키를 저장하려면 백업이 권장되지만 키 파일의 수동 백업도 필요합니다.

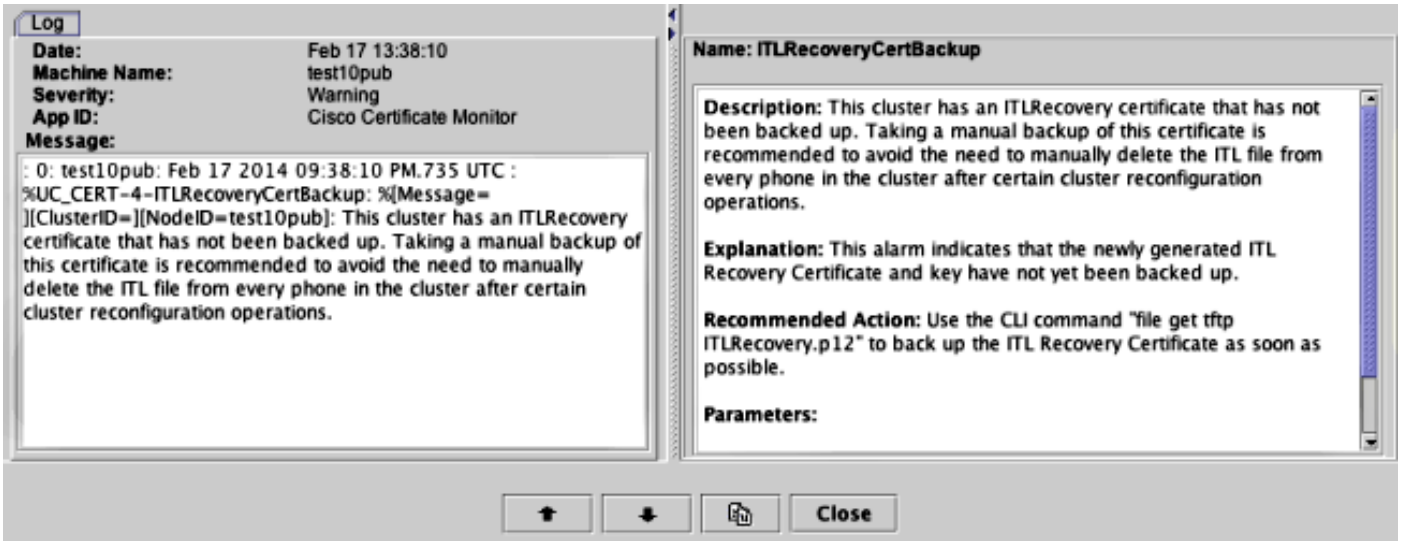
복구 키를 백업하려면 게시자의 CLI에 로그인하고 get tftp ITLRecovery.**p12** 명령 **파일을** 입력합니다.여기에 표시된 대로 파일을 저장하려면 SFTP 서버가 필요합니다.가입자 노드에는 ITL 복구 파일이 없으므로 **파일 get tftp ITLRecovery.p12** 명령을 구독자에서 실행하면 **파일을 찾을 수 없습니다**.

```
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 파일을 백업하기 위해 CLI에서 수동 백업을 수행할 때까지 CiscoSyslog(Event Viewer - Application Log)에 아래와 같이 경고가 매일 표시됩니다.OS Administration(OS 관리) 페이지, Security(**보안**) > Certificate Monitor(인증서 모니터)에서 이메일 알림이 활성화된 경우 수동 백업이 수행될 때까지 매일 이메일**을 받을** 수도 있습니다.



DRS 백업에 ITLRecovery가 포함되어 있는 경우에도 백업 파일이 손실되거나 손상되거나 백업에서 복원할 필요 없이 ITL 파일을 재설정할 수 있는 옵션이 있는 경우 ITLRecovery.p12 파일을 안전한 위치에 저장하는 것이 좋습니다.게시자가 저장한 ITLRecovery.p12 파일이 있는 경우, DRS 복원 옵션을 사용하여 가입자에서 데이터베이스를 복원하고 utils itl reset remotekey 옵션으로 ITL을 재설정하여 폰과 CUCM 서버 간의 신뢰를 다시 설정하는 백업 없이 게시자를 다시 작성할 수 있습니다.

게시자가 다시 작성되면 클러스터 보안 비밀번호는 ITLRecovery.p12 파일이 클러스터 보안 비밀번호를 기반으로 비밀번호로 보호되어 있으므로 ITLRecovery.p12 파일이 가져온 게시자와 동일해야 합니다.따라서 클러스터 보안 암호가 변경되면 ITLRecovery.p12 파일이 백업되지 않았음을 나타내는 RTMT 알림이 재설정되고 새 ITLRecovery.p12 파일이 get tftp ITLRecovery.p12 **파일**과 함께 저장될 때까지 매일 트리거됩니다.

다음을 확인합니다.

벌크 ITL 재설정 기능은 전화기에 ITLRecovery 항목이 포함된 ITL이 설치된 경우에만 작동합니다.전화기에 설치된 ITL 파일에 ITLRecovery 항목이 포함되어 있는지 확인하려면 각 TFTP 서버의 CLI에서 **show itl** 명령을 입력하여 ITL 파일의 체크섬을 찾습니다.show itl 명령의 출력**에** 체크섬이 표시됩니다.

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

각 서버에는 ITL 파일에 자체 callmanager**.pem** 인증서가 있으므로 체크섬은 각 TFTP 서버마다 다릅니다.전화기에 설치된 ITL의 ITL 체크섬은 Settings(설정) **> Security Configuration(보안 컨피그레이션) > Trust List(신뢰 목록)**의 전화기 또는 전화기 웹 페이지에서 또는 최신 펌웨어를 실행하는 전화기에서 보고된 DeviceTLInfo 알람에서 확인할 수 있습니다.

펌웨어 버전 9.4(1) 이상을 실행하는 대부분의 전화기는 ITL의 SHA1 해시를 DeviceTLInfo 경보와 함께 CUCM에 보고합니다.전화기가 전송하는 정보는 이벤트 뷰어 - RTMT의 애플리케이션 로그에서 볼 수 있으며, 전화기가 현재 ITL이 설치되지 않은 ITL을 포함하는 전화기를 찾기 위해 사용하는 TFTP 서버의 ITL 해시의 SHA1 해시와 비교할 수 있습니다.

주의 사항

- CSCun18578 - 특정 시나리오에서 ITL reset localkey/remotekey가 실패합니다.
- CSCun19112 - SFTP 잘못된 인증 유형의 ITL 재설정 remotekey 오류