统一通信管理器在版本10.0(1)的ITL增强

目录

简介

本文描述在启用标识信任在Cisco Unified IP电话的列表的Cisco Unified Communications Manager (CUCM)版本10.0(1)的一新特性(ITL)文件大批重置。使用容量ITL重置功能，当电话不再委托ITL文件签署人并且不能验证ITL文件带有由TFTP服务本地或使用托拉斯验证服务时(TV)。

背景

能力变大块重置ITL文件防止需要执行这些步骤之一或许多重建在IP电话和CUCM服务器之间的信任。

- 从备份的恢复为了上传电话委托的一个旧有ITL文件
- 更换电话为了使用一不同的TFTP server
- 通过Settings菜单手工删除从电话的ITL文件
- 出厂重置在事件设置的电话，以便访问禁用为了清除ITL

此功能没有打算移动电话在集群之间;对于该任务，请使用描述的其中一个方法在移植IP电话在集群之间用CUCM 8和ITL文件。当他们下跌了他们的信任点时， ITL重置操作用于只重建在IP电话和CUCM集群之间的信任。

在本文没有报道的CUCM版本10.0(1)的另一与安全相关的功能联机是Tokenless Certficate信任列表(CTL)。Tokenless CTL用用于的软件标记替换硬件USB安全令牌为了启用在CUCM服务器和终端的加密。其他信息，参考IP电话安全和CTL (证书信任列表)文档。

关于ITL文件的默认情况下其他信息和安全可以在通信管理器安全找到默认情况下和ITL操作和故障排除文档。

问题症状

当电话在**已锁定**或**不信任的状态时**，他们不接受TFTP服务或TFTP配置提供的ITL文件。在TFTP配置文件包含的任何配置更改没有应用对电话。在TFTP配置文件包含设置的某些示例是：

- 设置访问
- Web 访问
- 安全壳SSH访问
- 对PC端口的交换端口分析器(SPAN)

如果这些设置中的任一为在CCM管理员页面的一个电话，在电话重置后，更改更改请勿生效，电话也许不委托TFTP server。另一常见的症状是，当您访问公司目录或其他电话服务时，消息**主机没找到的**显示。为了验证电话在已锁定或不信任的状态，是否请检查从电话的电话状态消息或电话网页为了发现**托拉斯列表更新失败消息**显示。**ITL更新失败消息**是指示器电话在已锁定或不信任的状态，因为失败验证与其当前ITL的信任列表并且失败验证它与TV。

如果导航对**设置>状态>状态消息，托拉斯列表更新失败消息**能从电话被看到：

托拉斯列表更新失败消息能从从**状态消息的**电话网页也被看到如显示此处：

解决方案-大批ITL重置

CUCM版本10.0(1)使用能使用为了重建在电话和CUCM服务器之间的信任的一另外的密钥。此新密钥是ITL恢复密钥。在安装或升级期间， ITL恢复密钥创建。此恢复密钥不更改，当主机名更改，DNS更改，或者也许导致问题电话进入状态他们不再委托他们的配置文件的签署人的其他更改执行。

新**使用情况itl重置的**CLI命令可以用于为了重建在电话或电话之间的信任和在CUCM的TFTP服务，当电话是在**信任列表更新失败消息**被看到的状态时。**reset命令使用情况的itl** ：

1. 采取从发行商节点的当前ITL文件，剥离签名ITL文件，并且再签署ITL文件的内容与ITL恢复专用密钥。
2. 自动地复制新的ITL文件对在所有的TFTP目录在集群的活动TFTP节点。
3. 自动地重新启动在TFTP运行的每个节点的TFTP服务。

管理员必须然后重置所有电话。重置造成电话请求ITL文件从TFTP server启动，并且ITL文件电话接收由ITLRecovery密钥签字而不是**callmanager.pem专用密钥**。有两个选项运行重置的ITL ：utilsitl**重置localkey和**utilsitl**重置remotekey。**reset命令的ITL可能从发行商只运行。如果发出从用户重置的ITL，导致Thisis**不是发行商Message节点**。每命令示例在以下部分被选派。

与本地恢复密钥的ITLRecovery

localkey选项在ITLRecovery.p12文件使用包含的ITL恢复专用密钥在发行商硬盘驱动器，新的ITL文件签署人。

```
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
```

与远程恢复密钥的ITLRecovery

remotekey选项允许ITLRecovery.p12文件保存指定的外部SFTP服务器。

```
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
```

> **注意**：如果ITL重置完成与remotekey选项， localkey (在磁盘文件)在发行商用remotekey替换。

验证当前签署人用“显示itl”命令

如果查看ITL文件用**显示itl**命令，在您发出reset命令前的ITL，显示ITL包含**ITLRECOVERY_ <** ***publisher_hostname - >***条目。由在集群的所有TFTP server服务的每个ITL文件包含从发行商的此ITL恢复条目。**显示itl**命令的输出从在本例中的发行商被采取。用于的标记为了签署ITL在粗体：

```
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.
```

验证使用ITLRecovery密钥

如果查看ITL文件用**显示itl**命令，在您执行ITL重置后，显示ITLRecovery条目签署了ITL如显示此处。ITLRecovery保持ITL的签署人，直到TFTP重新启动，那时**callmanager.pem**或TFTP证书用于为了再签署ITL。

```
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.
```

减小失去信任的电话的可能性的增强

除ITL重置功能之外，CUCM版本10.0(1)包括帮助防止电话输入不信任的状态的管理员功能。两信任指向电话有是TV证书(**TVS.pem)和**TFTP证书(callmanager.pem**)。在最**简单的环境用一个CUCM服务器，如果管理员重新生成callmanager.pemcertificate和TVS.pem证书一在别的之后，电话重置和启动后只显示托拉斯列表**更新失败消息。**与从CUCM发送的自动装置重置到电话由于在被重新生成的ITL包含的证书，电话能进入不委托CUCM的状态。

为了帮助防止多份证书同时被重新生成的方案(典型地主机名更改或DNS域名修改)，CUCM当前有一保持计时器。当证书被重新生成时，CUCM防止管理员重新生成在同一个节点的另一证书在上一个证书重新生成的五分钟内。此进程造成电话重置在重新生成第一证书，并且他们应该备份和已注册，在下证书被重新生成前。

不管哪证书首先生成，电话有验证其附属的方法文件。关于此进程的其他详细信息可以在通信管理器安全找到默认情况下和ITL操作和故障排除。

此输出显示情况CUCM在一上一个证书重新生成的五分钟内防止管理员重新生成另一证书观察从CLI的地方：

```
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
```

同一个消息能从操作系统(OS)管理页面被看到如显示此处：

发行商ITL恢复密钥是只那个在使用中由整个集群，即使每个节点有其自己的ITLRecovery证书发出对**ITLRecovery_ *<node name>***共同名称(CN)。发行商ITLRecovery密钥是用于ITL文件的只那个整个集群如被看到从**显示itl**命令。这就是为什么在ITL文件看到的唯一的**ITLRecovery_ *<hostname>***条目包含发行商的主机名。

如果发行商的主机名更改，在ITL的ITLRecovery条目继续显示发行商的旧有主机名。因为ITLRecovery文件不应该更改总是保证电话信任ITL恢复，这故意地执行。

当域名也是时，更改这申请;原始域名在ITLRecovery条目被看到为了保证恢复密钥不更改。当ITLRecovery证书应该更改是，当超时由于五年正确性之时，并且必须重新生成。

ITL恢复密钥对可以重新生成与CLI或OS管理页面。当ITLRecovery证书在发行商或被重新生成任何用户时， IP电话没有重置。一旦ITLRecovery证书被重新生成了， ITL文件不更新，直到TFTP服务重新启动。在ITLRecovery在发行商的证书重新生成以后，请重新启动在运行在集群的TFTP服务为了更新在ITL文件的ITLRecovery条目有新证书的每个节点的TFTP服务。最后一步将重置从**System > Enterprise Parameters的**所有设备和使用reset按钮为了做所有设备下载包含新的ITLRecovery证书的新的ITL文件。

备份ITL恢复

当他们进入不信任的状态时， ITL恢复密钥要求为了恢复电话。由于此，新建的实时监控工具(RTMT)警报是生成的日报，直到ITL恢复密钥备份。灾难恢复系统(DR)备份不足够了终止警报。虽然推荐备份为了保存ITL恢复密钥，关键文件的一个手动备份必要。

为了备份恢复密钥，登录到发行商的CLI和输入**文档获得tftp ITLRecovery.p12**命令。SFTP服务器是需要的为了保存文件对如显示此处。用户节点没有一个ITL恢复文件，因此，如果发出**文件获得tftp ITLRecovery.p12** on命令用户，它导致没**找到的文件**。

```
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
```

直到手动备份从CLI执行为了备份ITLRecovery.p12文件，警告在CiscoSyslog (事件浏览器应用程序日志)每天打印如显示此处。一每天电子邮件也许也接收，直到手动备份执行，如果电子邮件通知从OS管理页面启用，**安全>证书箴言报**。

当DR备份包含ITLRecovery时，在一个安全位置推荐仍然存储ITLRecovery.p12文件，万一备份文件丢失或毁损或者为了有选项重置ITL文件，不用需要从备份恢复。如果有从发行商的ITLRecovery.p12文件保存，也允许将重建的发行商，不用一个备份以使用DR Restore选项恢复从susbcriber的数据库和重建在电话和CUCM服务器之间的信任通过重置与**使用情况itl重置remotekey**选项的ITL。

切记，如果发行商重建，集群安全密码应该是相同的象ITLRecovery.p12文件被采取从的发行商，因为ITLRecovery.p12文件是密码保护的与密码根据集群安全密码。为此，如果集群安全密码更改，指示的RTMT警报ITLRecovery.p12文件未备份重置并且触发日报，直到新的ITLRecovery.p12文件用**文件**保存**获得tftp ITLRecovery.p12**命令。

验证

容量ITL重置功能只运作，如果电话有包含ITLRecovery条目安装的ITL。为了验证在电话安装的ITL文件包含ITLRecovery条目，请输入从CLI的**显示itl**命令在其中每一个TFTP服务器查找ITL文件的校验和。从**显示itl**命令的输出显示校验和：

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

因为每个服务器有其自己的**callmanager.pem证书**在其ITL文件，校验和是不同的在每TFTP server。可以找到在电话安装的ITL的ITL校验和是否查看在电话的ITL在设置**> Security Configuration>托拉斯列表下，从**电话网页，或者从运行新的固件的电话报告的DeviceTLInfo报警。

送固件版本9.4(1)或以上报告他们的ITL SHA1哈希到CUCM用DeviceTLInfo报警的多数电话。电话发送的信息在从RTMT的事件浏览器应用程序日志可以查看和与TFTP服务器的ITL哈希的SHA1哈希比较电话使用为了查找没有安装的当前ITL，包含ITLRecovery条目的所有电话。

警告

- CSCun18578 -在某些情况下ITL重置localkey/remotekey发生故障
- CSCun19112 - ITL重置在SFTP未成功认证类型的remotekey错误