使用无令牌 CTL 的 CUCM 混合模式

目录

简介

本文档介绍使用/不使用硬件USB eTokens的Cisco Unified Communications Manager(CUCM)安全性之间的差异。

先决条件

要求

思科建议您了解 CUCM 版本 10.0(1) 或更高版本的知识。此外，请确保：

- CUCM 版本 11.5.1SU3 及更高版本的许可证服务器必须使用 Cisco Prime License Manager (PLM) 11.5.1SU2 或更高版本。

这是因为 CUCM 版本 11.5.1SU3 需要加密许可证才能启用混合模式，而版本 11.5.1SU2 之前的 PLM 不支持加密许可证。

有关详细信息，请参阅 Cisco Prime License Manager 版本 11.5(1)SU2 的发行说明。

- 您拥有对 CUCM 发布方节点命令行界面 (CLI) 的管理访问权限。
- 您可以访问硬件 USB 电子令牌，并且 PC 上已安装 CTL 客户端插件，用于需要重新迁移到使用硬件电子令牌的场景。

为了更清晰地了解，此要求仅当您在任何时候都有一个需要USB eToken的场景时才适用。大多数人都需要USB eToken的可能性很小。

- 集群中所有 CUCM 节点之间都有完全的连通性。这一点非常重要，因为 CTL 文件将通过 SSH 文件传输协议 (SFTP) 复制到集群中的所有节点。
- 集群中的数据库 (DB) 复制正常工作，并且服务器会实时复制数据。
- 部署中的设备支持默认安全设置 (TVS)。

您可以使用”Cisco Unified Reporting”网页 (https://<CUCM IP or FQDN>/cucreports/) 中的 Unified CM 电话功能列表，来确定支持默认安全设置的设备。

注意：默认情况下，Cisco Jabber和许多Cisco TelePresence或Cisco 7940/7960系列IP电话当前不支持安全功能。如果您使用默认情况下不支持安全的设备部署无令牌的CTL，则在发布服务器上更改CallManager证书的任何系统更新都将阻止这些设备的正常功能，直到手动删除CTL。支持默认安全设置的设备（例如 7945 和 7965 系列电话或更新型号）能够在更新发布方的 CallManager 证书时安装 CTL 文件，因为它们可以使用信任验证服务 (TVS)。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CUCM 版本 10.5.1.10000-7（两个节点的集群）
- 使用固件版本 SCCP75.9-3-1SR4-1S 通过瘦客户端控制协议 (SCCP) 注册的思科 7975 系列 IP 电话
- 两个思科安全令牌，用于借助 CTL 客户端软件将集群设置为混合模式

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档介绍在使用和不使用硬件 USB 电子令牌的情况下 Cisco Unified Communications Manager (CUCM) 安全性之间的差异。

本文档还介绍了涉及无令牌证书信任列表 (CTL) 的基本实施方案，以及用于确保系统在更改后正常运行的过程。

无令牌 CTL 是 CUCM 版本 10.0(1) 及更高版本中的一项新功能，无需使用以往 CUCM 版本必需的硬件 USB 电子令牌和 CTL 客户端插件，即可对 IP 电话的呼叫信令和媒体进行加密。

使用 CLI 命令将集群置于混合模式时，系统将使用发布方节点的 CCM+TFTP（服务器）证书对 CTL 文件进行签署，并且 CTL 文件中没有电子令牌证书。

注意：在发布服务器上重新生成CallManager(CCM+TFTP)证书时，它会更改文件的签名人。默认情况下不支持安全功能的电话和设备也不接受新的CTL文件，除非从每台设备上手动删除CTL文件。有关详细信息，请参阅本文档 Requirements（要求）部分中列出的最后一个要求。

从非安全模式迁移到混合模式（无令牌 CTL）

本节介绍用于通过 CLI 将 CUCM 集群安全移至混合模式的过程。

在此场景之前，CUCM 处于非安全模式，这表示任何节点上均不存在 CTL 文件，并且所注册的 IP 电话仅安装了身份信任列表 (ITL) 文件，如以下输出所示：

<#root>

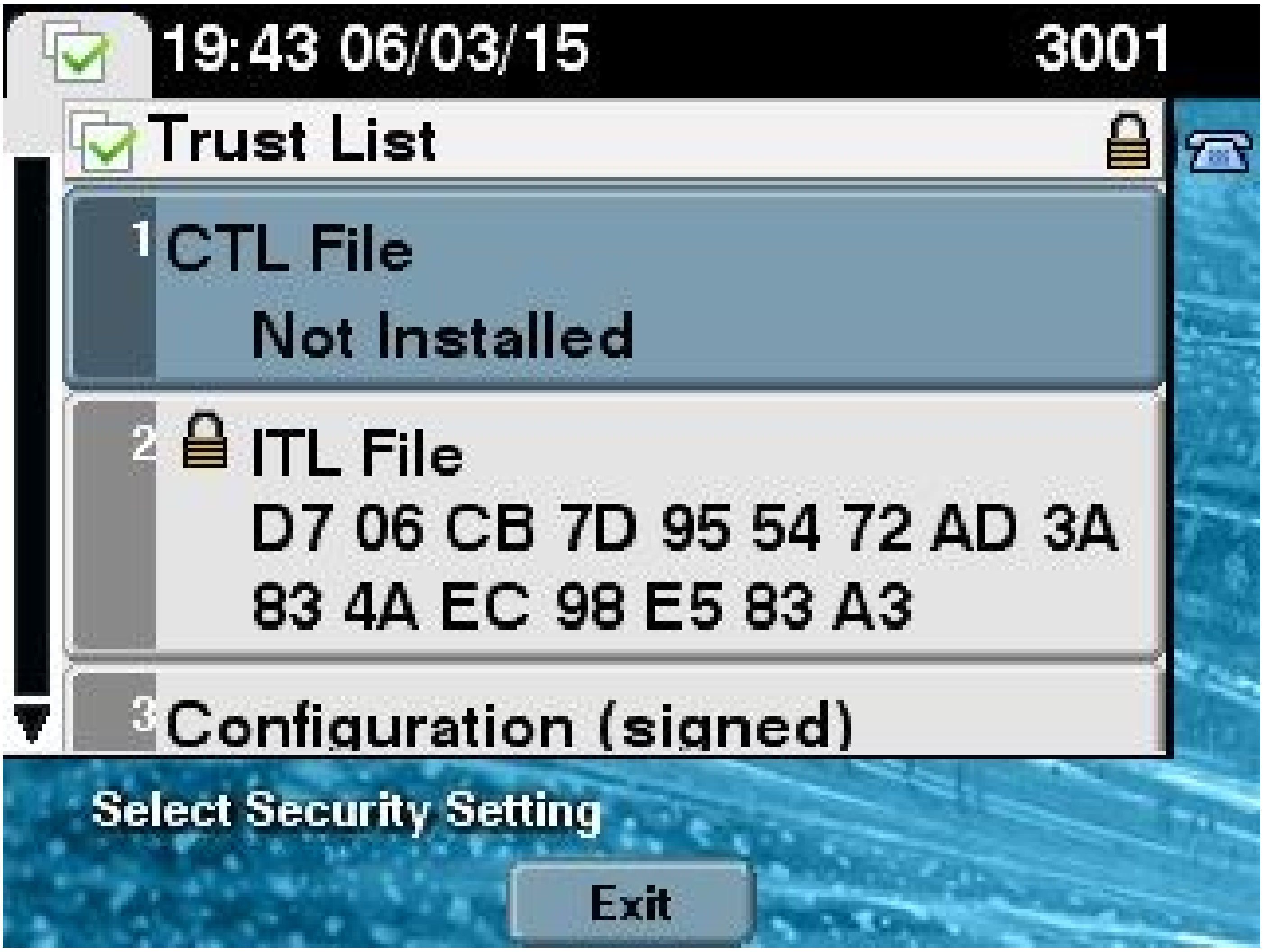
```
admin:

show ctl

Length of CTL file: 0

CTL File not found

. Please run CTLClient plugin or run the CLI - utils ctl.. to
 generate the CTL file.
Error parsing the CTL File.
admin:
```

注：如果当群集未处于混合模式时，在服务器上找到一个CTL文件，这意味着群集曾经处于混合模式，然后移回非混合模式，并且CTL文件没有从群集中删除。

命令file delete activelog cm/tftpdata/CTLFile.tlv从CUCM集群中的节点中删除CTL文件；但是，需要在每个节点上输入该命令。需要明确的是，仅在服务器具有 CTL 文件且集群未处于混合模式时使用此命令。

确认集群是否处于混合模式的一种简单方法是使用命令 run sql select paramname,paramvalue from processconfig where paramname='ClusterSecurityMode'。如果参数值为 0，则集群不处于混合模式。

```
run sql select paramname,paramvalue from processconfig where paramname='ClusterSecurityMode'
paramname           paramvalue
=================== ==========
ClusterSecurityMode 0
```



19:43 06/03/15 3001

Trust List

1 CTL File
Not Installed

2 ITL File
D7 06 CB 7D 95 54 72 AD 3A
83 4A EC 98 E5 83 A3

3 Configuration (signed)

Select Security Setting

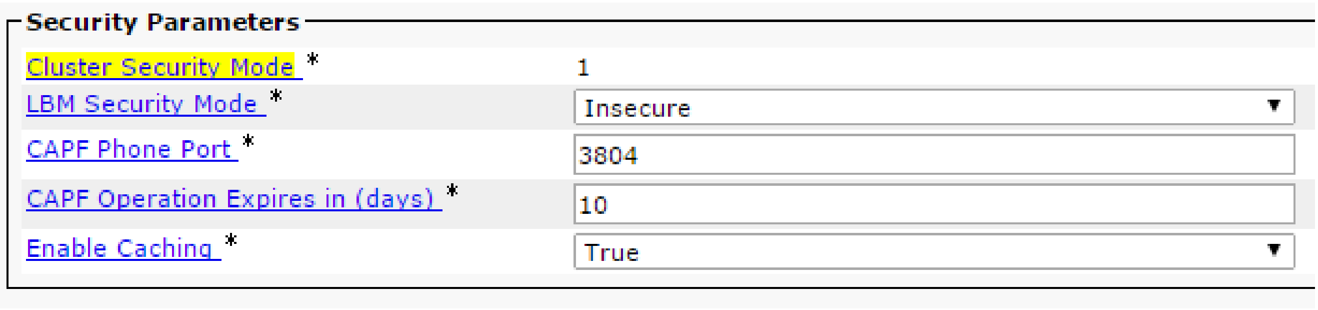
要使用全新的无令牌 CTL 功能将 CUCM 集群安全移至混合模式，请完成以下步骤：

1. 获取对 CUCM 发布方节点 CLI 的管理访问权限。

2. 在 CLI 中输入 utils ctl set-cluster mixed-mode 命令：

```
<#root>

admin:

utils ctl set-cluster mixed-mode


This operation sets the cluster to Mixed mode. Do you want to continue? (y/n):y

Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
Please Restart the TFTP and Cisco CallManager services on all nodes in the cluster
 that run these services
admin:
```

3. 导航至 CUCM Admin Page（CUCM 管理页面）> System（系统）> Enterprise Parameters（企业参数），并验证集群是否已设置为“混合”模式（值 1 表示“混合”模式）：



Security Parameters

Cluster Security Mode *	1
LBM Security Mode *	Insecure
CAPF Phone Port *	3804
CAPF Operation Expires in (days) *	10
Enable Caching *	True

4. 在运行这些服务的集群中的所有节点上，重新启动 TFTP 和 Cisco CallManager 服务。

5. 重新启动所有 IP 电话，以便它们可以从 CUCM TFTP 服务获取 CTL 文件。

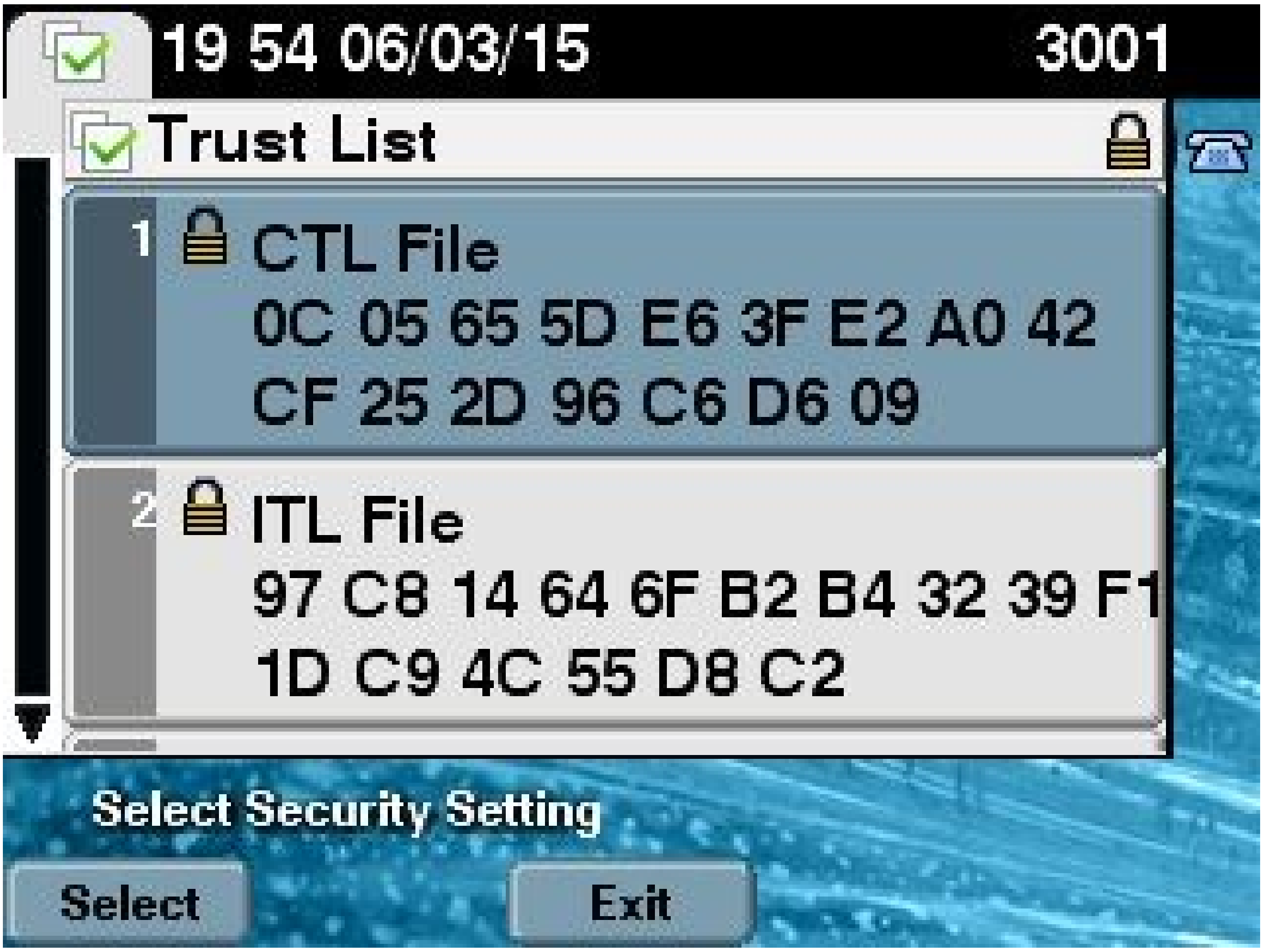
6. 要验证 CTL 文件的内容，请在 CLI 中输入 show ctl 命令。
7. 在 CTL 文件中，您可以看到 CUCM 发布方节点的 CCM+TFTP（服务器）证书用于签署 CTL 文件（此文件在集群中的所有服务器上均相同）。以下为示例输出：

```
<#root>

admin:

show ctl


The checksum value of the CTL file:

0c05655de63fe2a042cf252d96c6d609(MD5)


8c92d1a569f7263cf4485812366e66e3b503a2f5(SHA1)

Length of CTL file: 4947
The CTL File was last modified on Fri Mar 06 19:45:13 CET 2015


[...]



        CTL Record #:1
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1156
2       DNSNAME         16      cucm-1051-a-pub
3       SUBJECTNAME     62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
4       FUNCTION        2       System Administrator Security Token
5       ISSUERNAME      62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
6       SERIALNUMBER    16

70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB


7       PUBLICKEY       140
```

```
8       SIGNATURE       128
9       CERTIFICATE     694     E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21
                                A5 A3 8C 9C (SHA1 Hash HEX)
10      IPADDRESS       4

This etoken was used to sign the CTL file.


        CTL Record #:2
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1156
2       DNSNAME         16      cucm-1051-a-pub
3       SUBJECTNAME     62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
4       FUNCTION        2

CCM+TFTP


5       ISSUERNAME      62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
6       SERIALNUMBER    16

70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB


7       PUBLICKEY       140
8       SIGNATURE       128
9       CERTIFICATE     694     E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21
                                A5 A3 8C 9C (SHA1 Hash HEX)
10      IPADDRESS       4


[...]



The CTL file was verified successfully.
```

8. 在 IP 电话端，您可以验证服务重新启动后是否会下载 CTL 文件，该文件现在位于 TFTP 服务器上（与 CUCM 的输出相比，MD5 校验和匹配）：

注意：在验证电话上的校验和时，您会看到MD5或SHA1，具体取决于电话类型。



19 54 06/03/15 3001

Trust List

1 CTL File
0C 05 65 5D E6 3F E2 A0 42
CF 25 2D 96 C6 D6 09

2 ITL File
97 C8 14 64 6F B2 B4 32 39 F1
1D C9 4C 55 D8 C2

Select Security Setting

从硬件电子令牌迁移到无令牌解决方案

本节介绍如何将 CUCM 集群安全从硬件电子令牌迁移到使用新的无令牌解决方案。

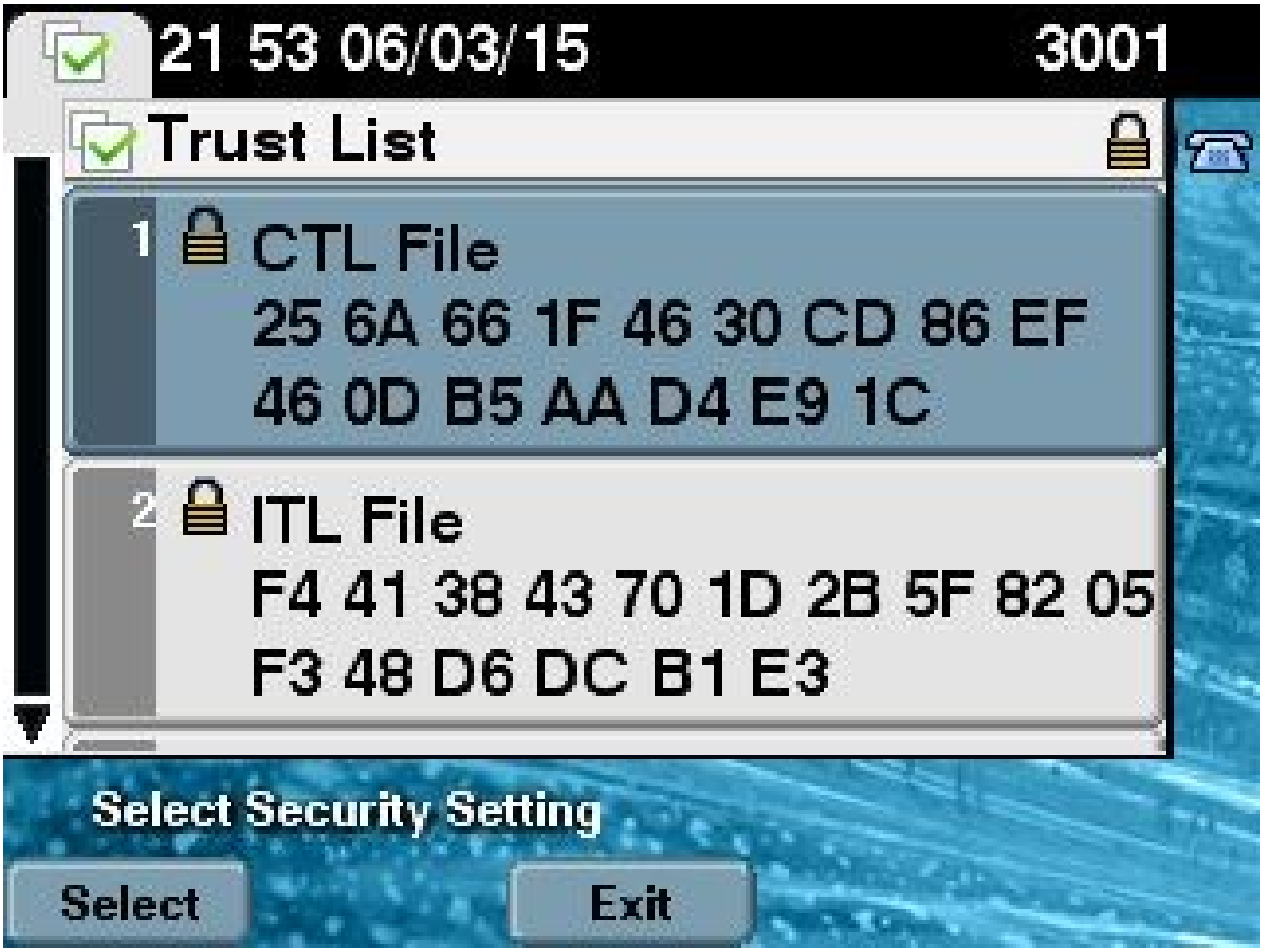
在某些情况下，已使用 CTL 客户端在 CUCM 上配置了混合模式，并且 IP 电话使用包含硬件 USB 电子令牌证书的 CTL 文件。

在这种情况下，CTL 文件由其中一个 USB 电子令牌的证书签署，并安装在 IP 电话上。在下面的示例中：

<#root>

```
admin:

show ctl


The checksum value of the CTL file:


256a661f4630cd86ef460db5aad4e91c(MD5)


3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
```

```
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015


[...]


        CTL Record #:5
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1186
2       DNSNAME         1
3       SUBJECTNAME     56      cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4       FUNCTION        2       System Administrator Security Token
5       ISSUERNAME      42      cn=Cisco Manufacturing CA;o=Cisco Systems
6       SERIALNUMBER    10

83:E9:08:00:00:00:55:45:AF:31


7       PUBLICKEY       140
9       CERTIFICATE     902     85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
                                3E 8B 3A 4F (SHA1 Hash HEX)
10      IPADDRESS       4

This etoken was used to sign the CTL file.



The CTL file was verified successfully.
```



21 53 06/03/15 3001

Trust List

1 CTL File
25 6A 66 1F 46 30 CD 86 EF
46 0D B5 AA D4 E9 1C

2 ITL File
F4 41 38 43 70 1D 2B 5F 82 05
F3 48 D6 DC B1 E3

Select Security Setting

完成以下步骤，以将 CUCM 集群安全转移到使用无令牌 CTL：

1. 获取对 CUCM 发布方节点 CLI 的管理访问权限。

2. 输入 utils ctl update CTLFile CLI 命令：

```
<#root>

admin:

utils ctl update CTLFile


This operation updates the CTLFile. Do you want to continue? (y/n):y

Updating CTL file
CTL file Updated
Please Restart the TFTP and Cisco CallManager services on all nodes in
 the cluster that run these services
```

3. 在运行这些服务的集群中的所有节点上，重新启动 TFTP 和 CallManager 服务。

4. 重新启动所有 IP 电话，以便它们可以从 CUCM TFTP 服务获取 CTL 文件。

5. 在 CLI 中输入 show ctl 命令，以验证 CTL 文件的内容。在 CTL 文件中，您可以看到 CUCM 发布方节点的 CCM+TFTP（服务器）证书将用于代替硬件 USB 电子令牌证书来签署 CTL 文件。
6. 在这种情况下，另一个重要区别在于，所有硬件 USB 电子令牌的证书均已从 CTL 文件中删除。以下为示例输出：

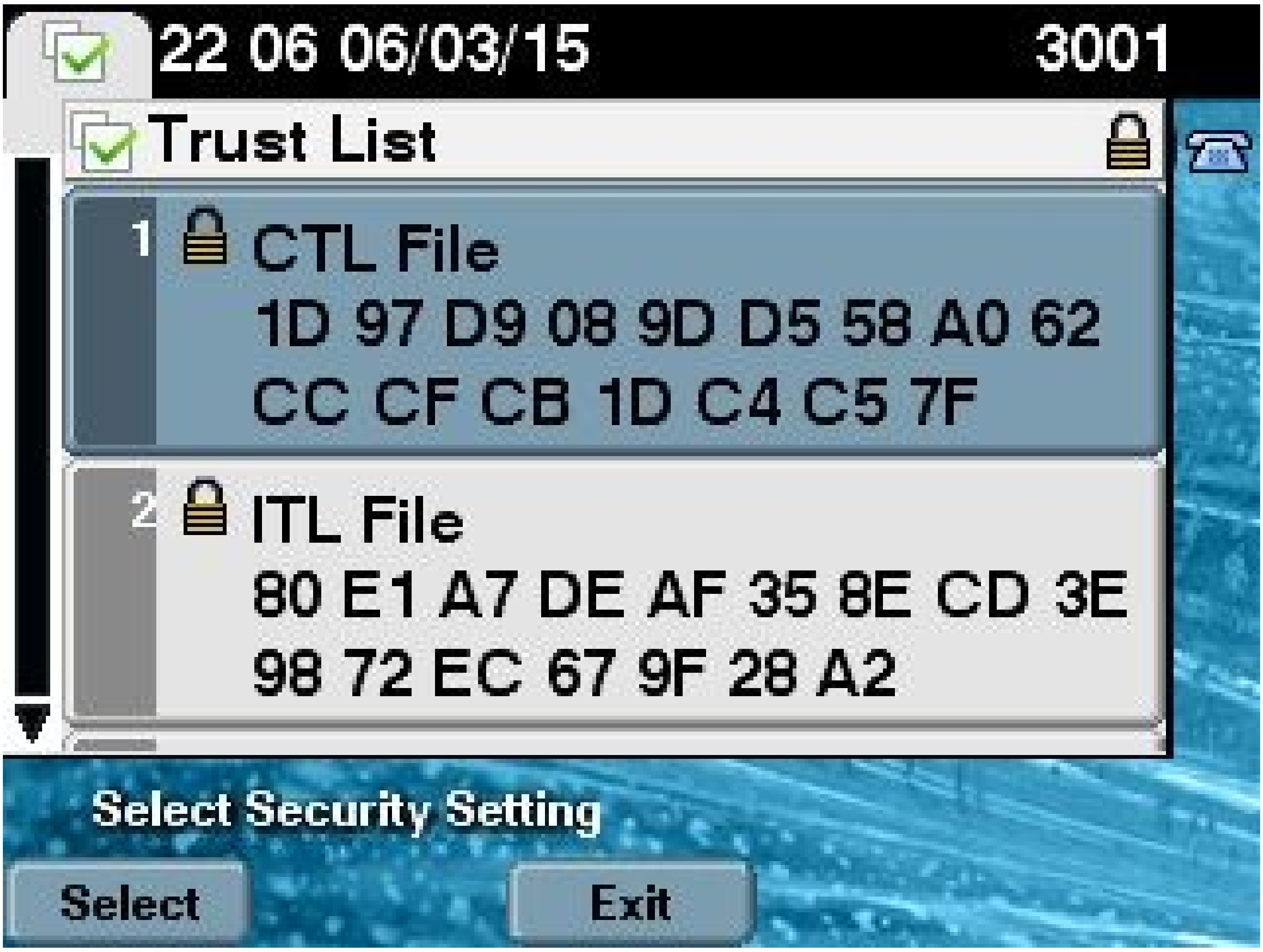
<#root>

```
admin:

show ctl


The checksum value of the CTL file:

1d97d9089dd558a062cccfcb1dc4c57f(MD5)


3b452f9ec9d6543df80e50f8b850cddc92fcf847(SHA1)

Length of CTL file: 4947
The CTL File was last modified on Fri Mar 06 21:56:07 CET 2015


[...]



CTL Record #:1
----
BYTEPOS TAG              LENGTH  VALUE
------- ---              ------  -----
1       RECORDLENGTH     2       1156
2       DNSNAME          16      cucm-1051-a-pub
3       SUBJECTNAME      62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                 ST=Malopolska;C=PL
4       FUNCTION         2

System Administrator Security Token


5       ISSUERNAME       62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                 ST=Malopolska;C=PL
6       SERIALNUMBER     16

 70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB


7       PUBLICKEY        140
8       SIGNATURE        128
9       CERTIFICATE      694     E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D
                                 21 A5 A3 8C 9C (SHA1 Hash HEX)
10      IPADDRESS        4

This etoken was used to sign the CTL file.



CTL Record #:2
----
```

```
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1156
2       DNSNAME         16      cucm-1051-a-pub
3       SUBJECTNAME     62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
4       FUNCTION        2

CCM+TFTP


5       ISSUERNAME      62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
6       SERIALNUMBER    16

70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB


7       PUBLICKEY       140
8       SIGNATURE       128
9       CERTIFICATE     694     E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D
                                21 A5 A3 8C 9C (SHA1 Hash HEX)
10      IPADDRESS       4

[...]


The CTL file was verified successfully.
```

注：在上述输出中，如果CUCM发布服务器的CCM+TFTP（服务器）证书未签名，则移回基于硬件令牌的集群安全模式，然后重新为无令牌解决方案重复更改。

7. 在 IP 电话端，您可以验证重新启动 IP 电话后是否已下载更新的 CTL 文件版本（与 CUCM 的输出相比，MD5 校验和匹配）：



22 06 06/03/15 3001

Trust List

1 CTL File
1D 97 D9 08 9D D5 58 A0 62
CC CF CB 1D C4 C5 7F

2 ITL File
80 E1 A7 DE AF 35 8E CD 3E
98 72 EC 67 9F 28 A2

Select Security Setting

从无令牌解决方案迁移到硬件电子令牌

本节介绍如何将 CUCM 集群安全从全新的无令牌解决方案重新迁移到使用硬件电子令牌。

使用 CLI 命令将 CUCM 集群安全设置为混合模式，并且使用 CUCM 发布方节点的 CCM+TFTP（服务器）证书签署 CTL 文件时，CTL 文件中没有硬件 USB 电子令牌证书。

因此，当您运行 CTL 客户端以更新 CTL 文件时（返回到使用硬件电子令牌）时，系统会显示以下错误消息：

```
The Security Token you have inserted does not exist in the CTL File
Please remove any Security Tokens already inserted and insert another
 Security Token. Click Ok when done.
```

这在以下情况中尤为重要：包括将系统降级（切换回该版本时）到不包含 utils ctl 命令的 10.x 之前的版本。

在刷新或从 Linux 升级到 Linux (L2) 的过程中，上一个 CTL 文件已迁移（不变更其内容），并且不包含电子令牌证书，如前所述。以下为示例输出：

<#root>

```
admin:

show ctl


The checksum value of the CTL file:

1d97d9089dd558a062cccfcb1dc4c57f(MD5)


3b452f9ec9d6543df80e50f8b850cddc92fcf847(SHA1)

Length of CTL file: 4947
The CTL File was last modified on Fri Mar 06 21:56:07 CET 2015

Parse CTL File
----------------

Version:        1.2
HeaderLength:   336 (BYTES)

BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
3       SIGNERID        2       149
4       SIGNERNAME      62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
5       SERIALNUMBER    16      70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB
6       CANAME          62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
7       SIGNATUREINFO   2       15
8       DIGESTALGORTITHM        1
9       SIGNATUREALGOINFO       2       8
10      SIGNATUREALGORTITHM     1
11      SIGNATUREMODULUS        1
12      SIGNATURE       128
65  ba  26  b4  ba  de  2b  13
b8  18  2  4a   2b  6c  2d  20
7d  e7  2f  bd  6d  b3  84  c5
bf  5   f2  74  cb  f2  59  bc
b5  c1  9f  cd  4d  97  3a  dd
6e  7c  75  19  a2  59  66  49
b7  64  e8  9a  25  7f  5a  c8
56  bb  ed  6f  96  95  c3  b3
72  7   91  10  6b  f1  12  f4
d5  72  e   8f  30  21  fa  80
bc  5d  f6  c5  fb  6a  82  ec
f1  6d  40  17  1b  7d  63  7b
52  f7  7a  39  67  e1  1d  45
b6  fe  82  0   62  e3  db  57
8c  31  2   56  66  c8  91  c8
d8  10  cb  5e  c3  1f  ef  a
14      FILENAME        12
15      TIMESTAMP       4

CTL Record #:1
----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1156
2       DNSNAME         16      cucm-1051-a-pub
3       SUBJECTNAME     62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
```

```
4       FUNCTION        2       System Administrator Security Token
5       ISSUERNAME      62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
6       SERIALNUMBER    16
```

70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB

```
7       PUBLICKEY       140
8       SIGNATURE       128
9       CERTIFICATE     694     E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D
                                21 A5 A3 8C 9C (SHA1 Hash HEX)
10      IPADDRESS       4
```

This etoken was used to sign the CTL file.

```
CTL Record #:2
----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1156
2       DNSNAME         16      cucm-1051-a-pub
3       SUBJECTNAME     62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
4       FUNCTION        2
```

CCM+TFTP

```
5       ISSUERNAME      62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
6       SERIALNUMBER    16
```

70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB

```
7       PUBLICKEY       140
8       SIGNATURE       128
9       CERTIFICATE     694     E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D
                                21 A5 A3 8C 9C (SHA1 Hash HEX)
10      IPADDRESS       4

CTL Record #:3
----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1138
2       DNSNAME         16      cucm-1051-a-pub
3       SUBJECTNAME     60      CN=CAPF-e41e7d87;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
4       FUNCTION        2       CAPF
5       ISSUERNAME      60      CN=CAPF-e41e7d87;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
6       SERIALNUMBER    16      74:4B:49:99:77:04:96:E7:99:E9:1E:81:D3:C8:10:9B
7       PUBLICKEY       140
8       SIGNATURE       128
9       CERTIFICATE     680     46 EE 5A 97 24 65 B0 17 7E 5F 7E 44 F7 6C 0A
                                F3 63 35 4F A7 (SHA1 Hash HEX)
10      IPADDRESS       4

CTL Record #:4
----
```

```
BYTEPOS TAG              LENGTH  VALUE
------- ---              ------  -----
1       RECORDLENGTH     2       1161
2       DNSNAME          17      cucm-1051-a-sub1
3       SUBJECTNAME      63      CN=cucm-1051-a-sub1;OU=TAC;O=Cisco;L=Krakow;
                                 ST=Malopolska;C=PL
4       FUNCTION         2       CCM+TFTP
5       ISSUERNAME       63      CN=cucm-1051-a-sub1;OU=TAC;O=Cisco;L=Krakow;
                                 ST=Malopolska;C=PL
6       SERIALNUMBER     16      6B:EB:FD:CD:CD:8C:A2:77:CB:2F:D1:D1:83:A6:0E:72
7       PUBLICKEY        140
8       SIGNATURE        128
9       CERTIFICATE      696     21 7F 23 DE AF FF 04 85 76 72 70 BF B1 BA 44
                                 DB 5E 90 ED 66 (SHA1 Hash HEX)
10      IPADDRESS        4

The CTL file was verified successfully.

admin:
```

对于这种情况，请完成以下步骤以安全地更新 CTL 文件，而无需使用丢失电子令牌的程序，此程序最终会从所有 IP 电话中手动删除 CTL 文件：

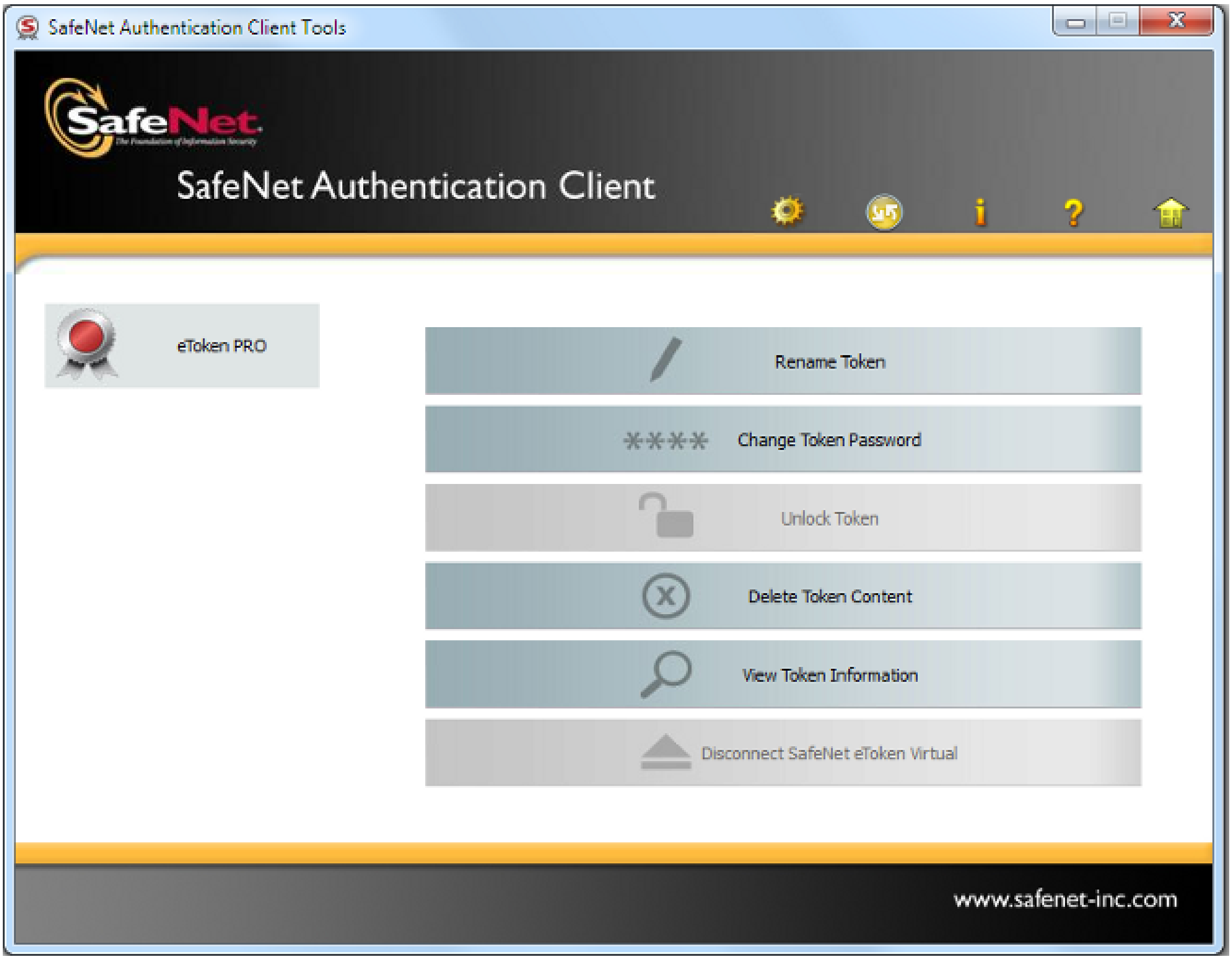
1. 获取对 CUCM 发布方节点 CLI 的管理访问权限。

2. 在发布方节点 CLI 中输入 file delete tftp CTLFile.tlv 命令，以删除 CTL 文件：

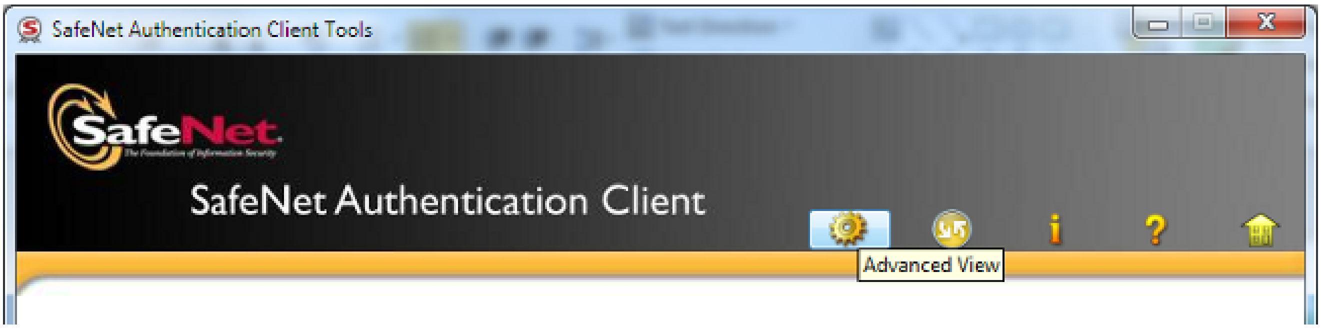
   <#root>

   ```
   admin:

   file delete tftp CTLFile.tlv


   Delete the File CTLFile.tlv?
   Enter "y" followed by return to continue: y
   files: found = 1, deleted = 1
   ```

3. 在已安装 CTL 客户端的 Microsoft Windows 计算机上，打开 SafeNet 身份验证客户端（它与 CTL 客户端一起自动安装）：

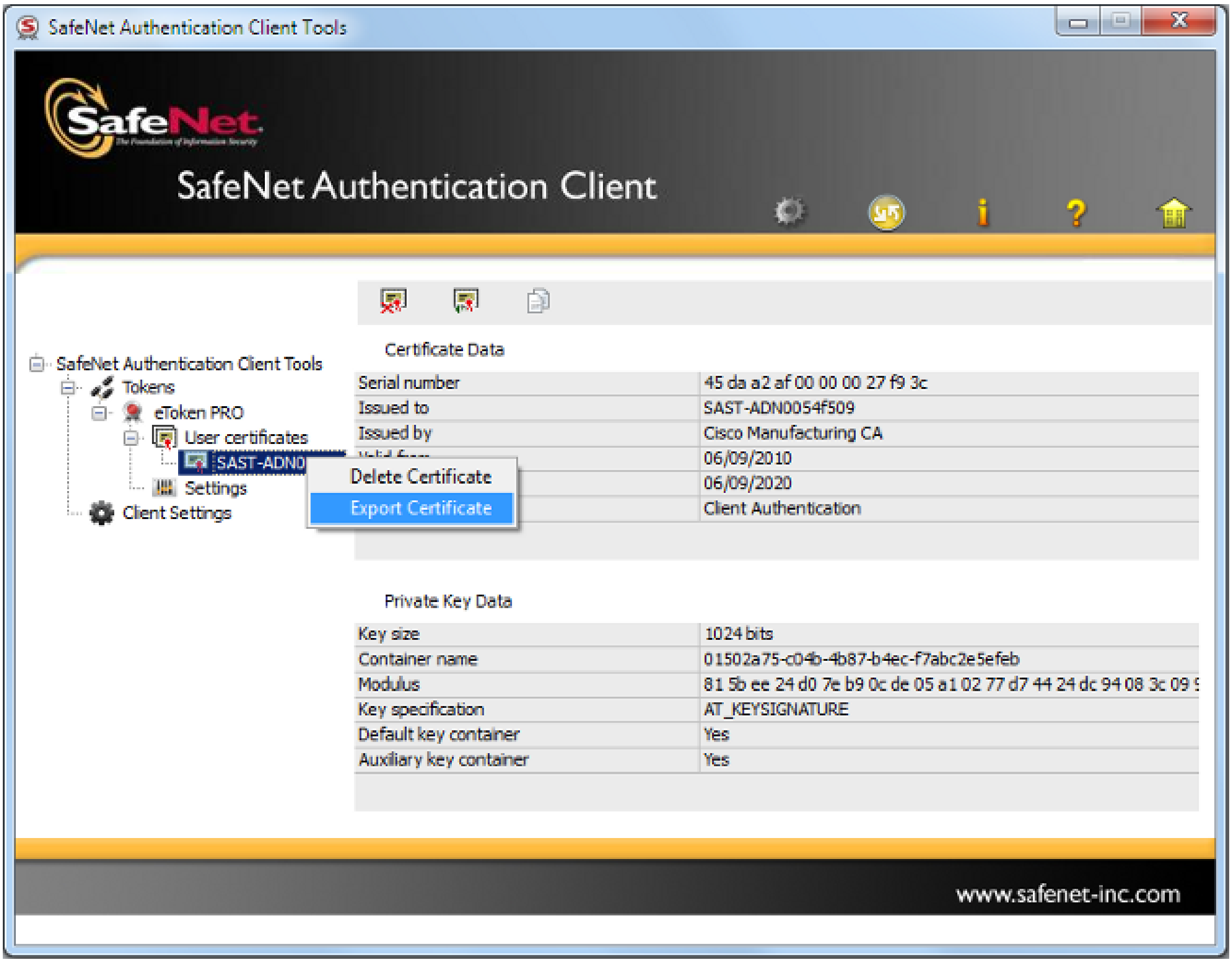


4. 在 SafeNet 身份验证客户端中，导航至 Advanced View（高级视图）：


SafeNet Authentication Client Tools
SafeNet
SafeNet Authentication Client
Advanced View

5. 插入第一个硬件 USB 电子令牌。

6. 选择 User certificates（用户证书）文件夹下的证书，然后将其导出到 PC 上的文件夹。当系统提示您输入密码时，请使用默认密码 Cisco123：



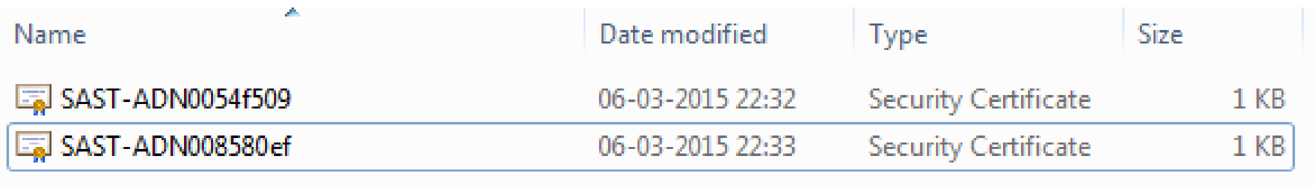
Certificate Data

Serial number	45 da a2 af 00 00 00 27 f9 3c
Issued to	SAST-ADN0054f509
Issued by	Cisco Manufacturing CA
Valid from	06/09/2010
	06/09/2020
	Client Authentication

Private Key Data

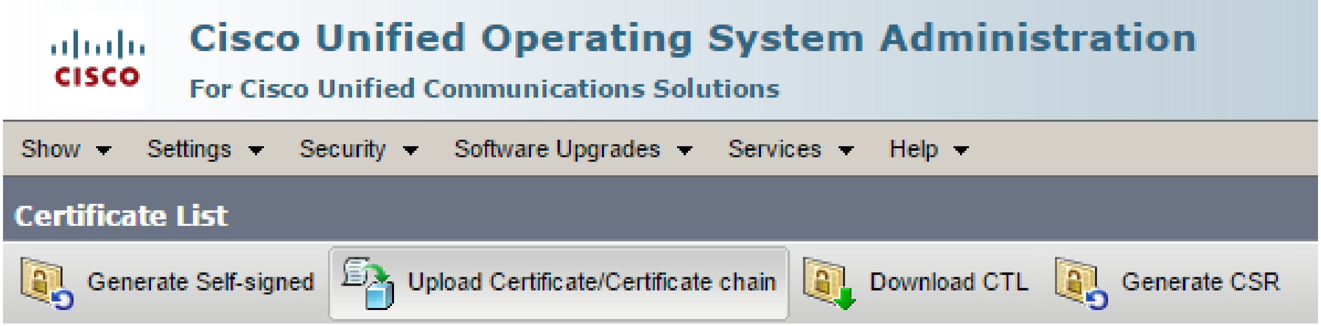
Key size	1024 bits
Container name	01502a75-c04b-4b87-b4ec-f7abc2e5efeb
Modulus	81 5b ee 24 d0 7e b9 0c de 05 a1 02 77 d7 44 24 dc 94 08 3c 09
Key specification	AT_KEYSIGNATURE
Default key container	Yes
Auxiliary key container	Yes

7. 对第二个硬件 USB 电子令牌重复这些步骤，以便将两个证书导出到 PC：

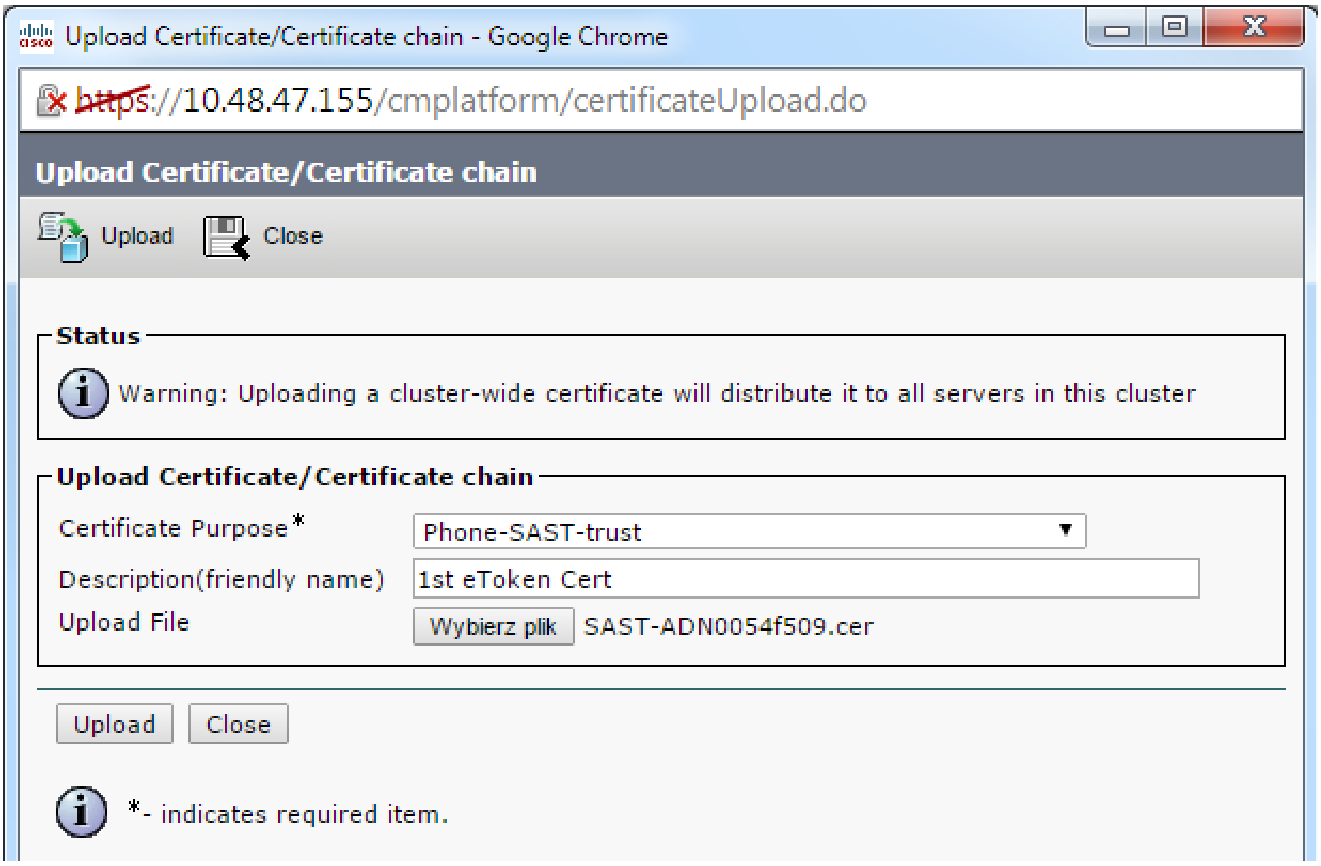


Name	Date modified	Type	Size
SAST-ADN0054f509	06-03-2015 22:32	Security Certificate	1 KB
SAST-ADN008580ef	06-03-2015 22:33	Security Certificate	1 KB

8. 登录到 Cisco Unified Operating System (OS) Administration 并导航至 Security（安全）> Certificate Management（证书管理）> Upload Certificate（上传证书）：


cisco
Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Show
Settings
Security
Software Upgrades
Services
Help
Certificate List
Generate Self-signed
Upload Certificate/Certificate chain
Download CTL
Generate CSR

9. 然后系统将显示“Upload Certificate”（上传证书）页面。从“Certificate Puepose”（证书用途）下拉菜单中选择 Phone-SAST-trust，然后选择从第一个电子令牌导出的证书：



Upload Certificate/Certificate chain - Google Chrome

https://10.48.47.155/cmplatform/certificateUpload.do

Upload Certificate/Certificate chain

Status

Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

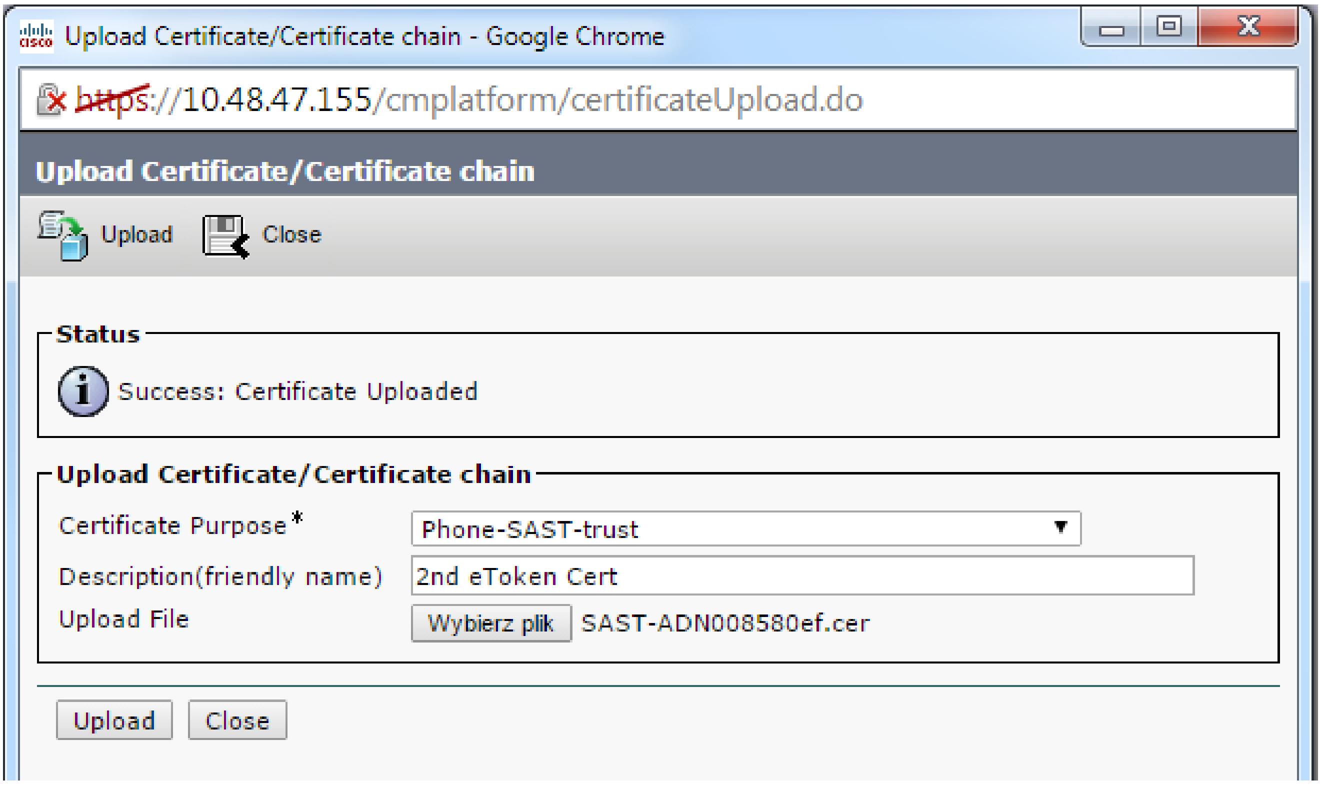
Certificate Purpose* Phone-SAST-trust

Description(friendly name) 1st eToken Cert

Upload File Wybierz plik SAST-ADN0054f509.cer

*- indicates required item.

10. 完成上述的步骤，以上传从第二个电子令牌导出的证书：



Upload Certificate/Certificate chain - Google Chrome

https://10.48.47.155/cmplatform/certificateUpload.do

Upload Certificate/Certificate chain

Status

Success: Certificate Uploaded

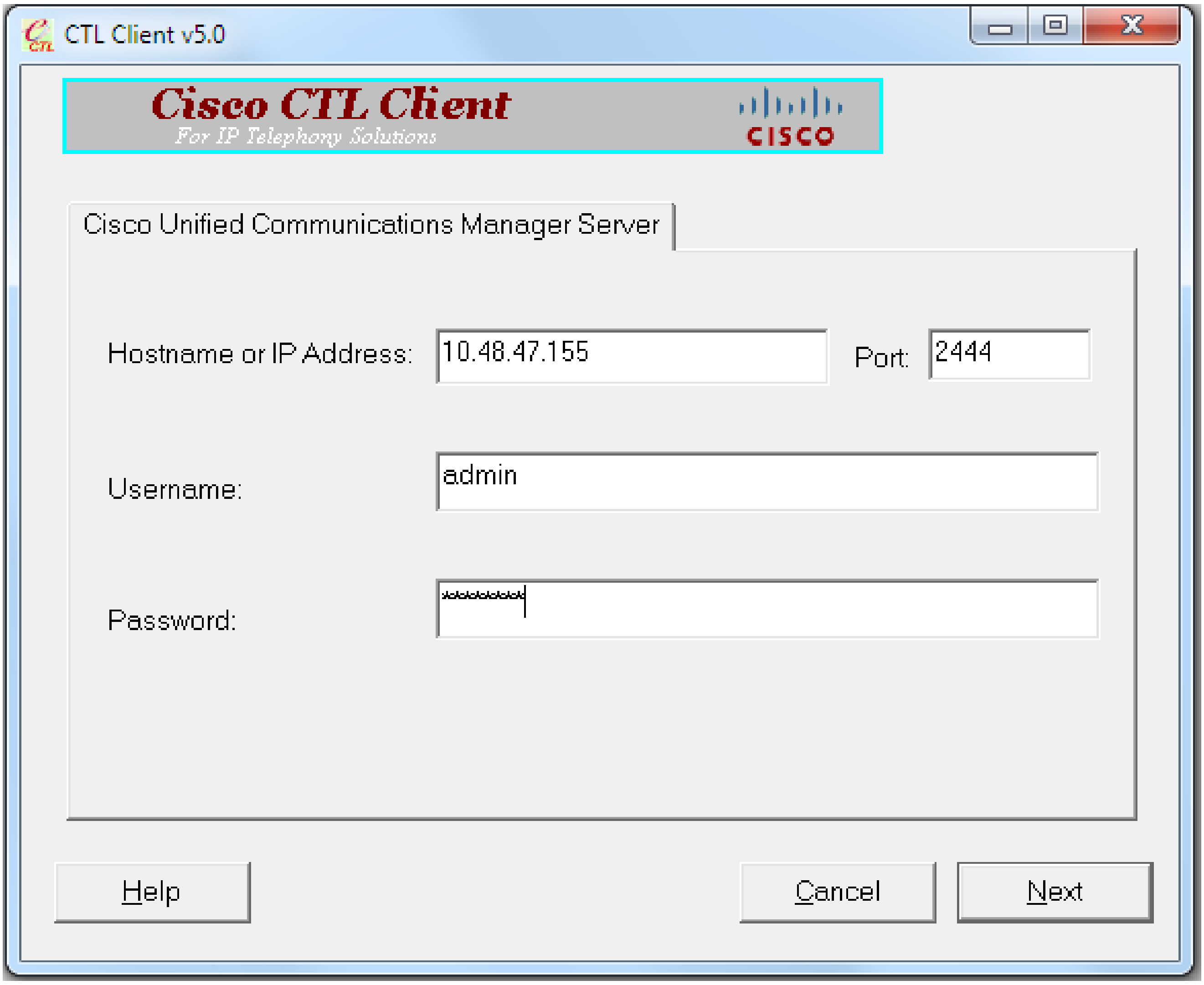
Upload Certificate/Certificate chain

Certificate Purpose* Phone-SAST-trust

Description(friendly name) 2nd eToken Cert

Upload File Wybierz plik SAST-ADN008580ef.cer

11. 运行 CTL 客户端，提供 CUCM 发布方节点的 IP 地址/主机名，然后输入 CCM 管理员凭证：


CTL Client v5.0
Cisco CTL Client
For IP Telephony Solutions
CISCO
Cisco Unified Communications Manager Server
Help
Cancel
Next

Hostname or IP Address: 10.48.47.155 Port: 2444

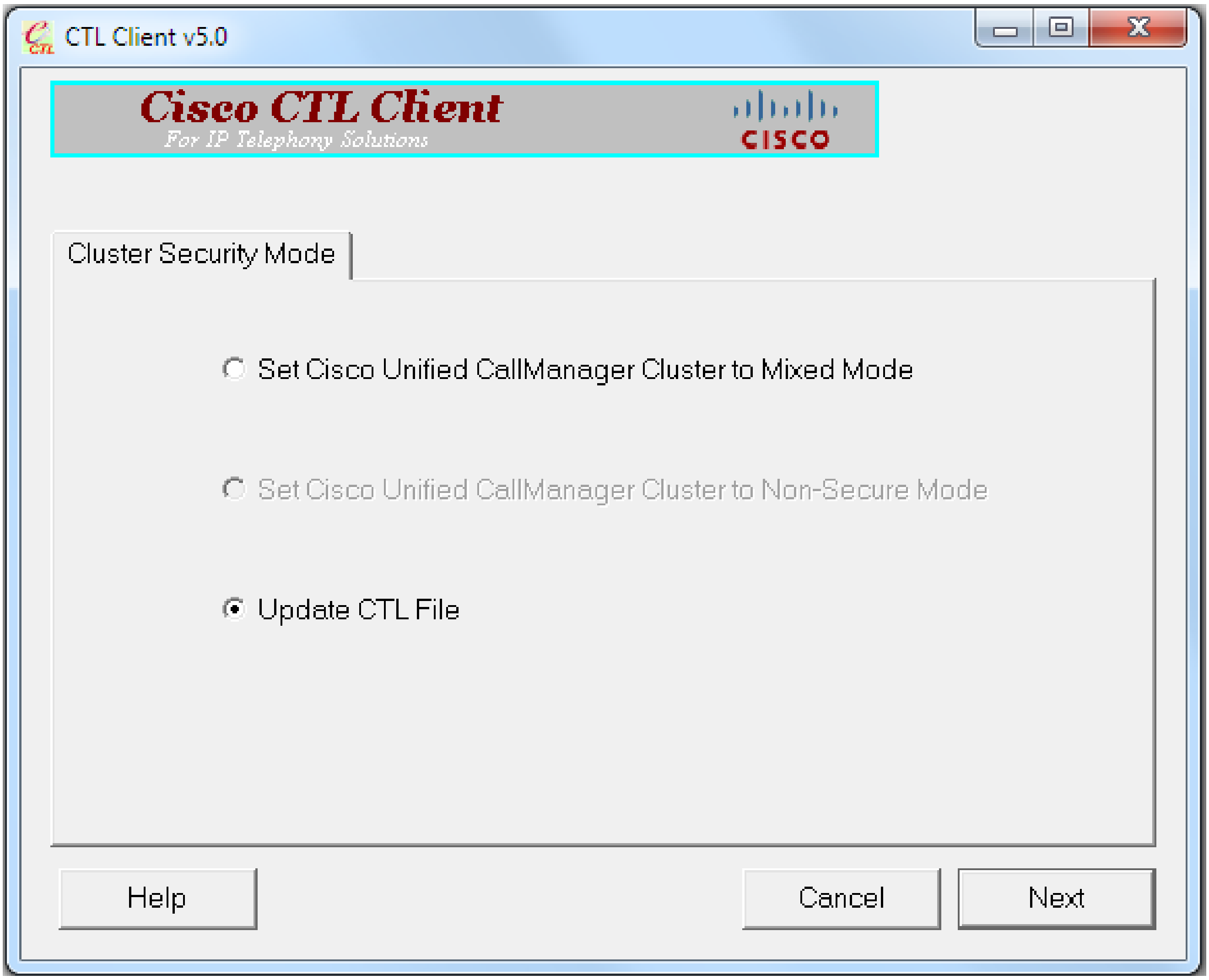
Username: admin

Password: ********

12. 由于集群已处于混合模式，但发布方节点上没有 CTL 文件，因此系统会显示以下警告消息（点击 OK（确定）忽略此消息）：

```
No CTL File exists on the server but the Call Manager Cluster Security Mode
 is in Secure Mode.
For the system to function, you must create the CTL File and set Call Manager
 Cluster the Secure Mode.
```

13. 在 CTL 客户端中，点击 Update CTL File（更新 CTL 文件）单选按钮，然后点击 Next（下一步）：



CTL Client v5.0

Cisco CTL Client
For IP Telephony Solutions

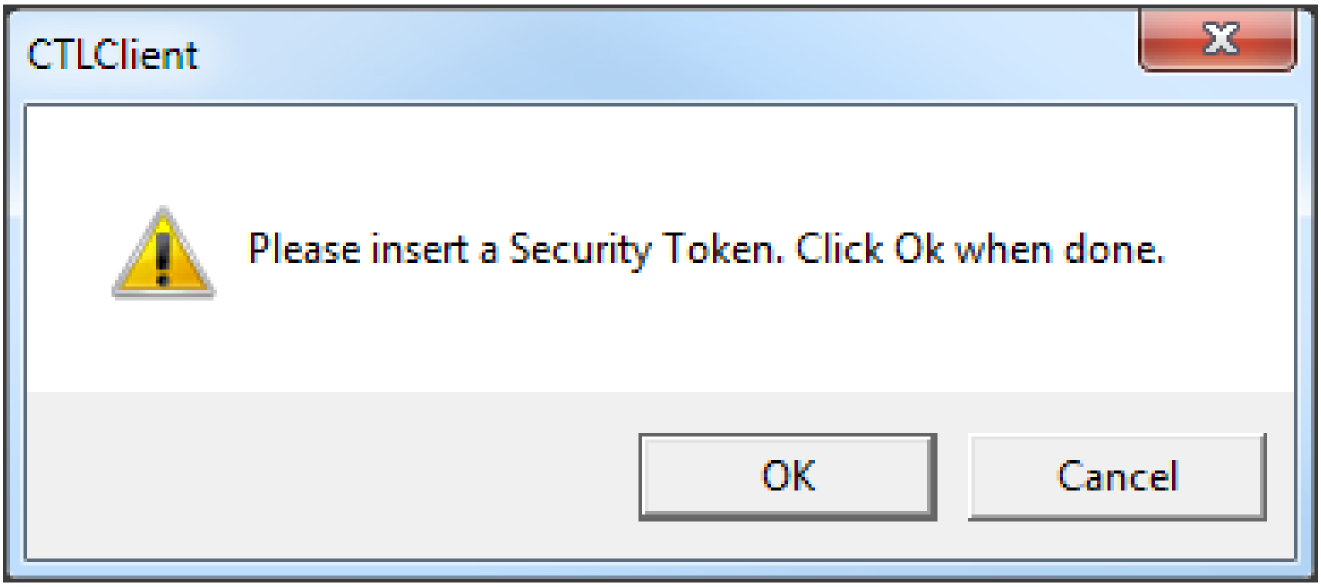
Cluster Security Mode

○ Set Cisco Unified CallManager Cluster to Mixed Mode

○ Set Cisco Unified CallManager Cluster to Non-Secure Mode

● Update CTL File

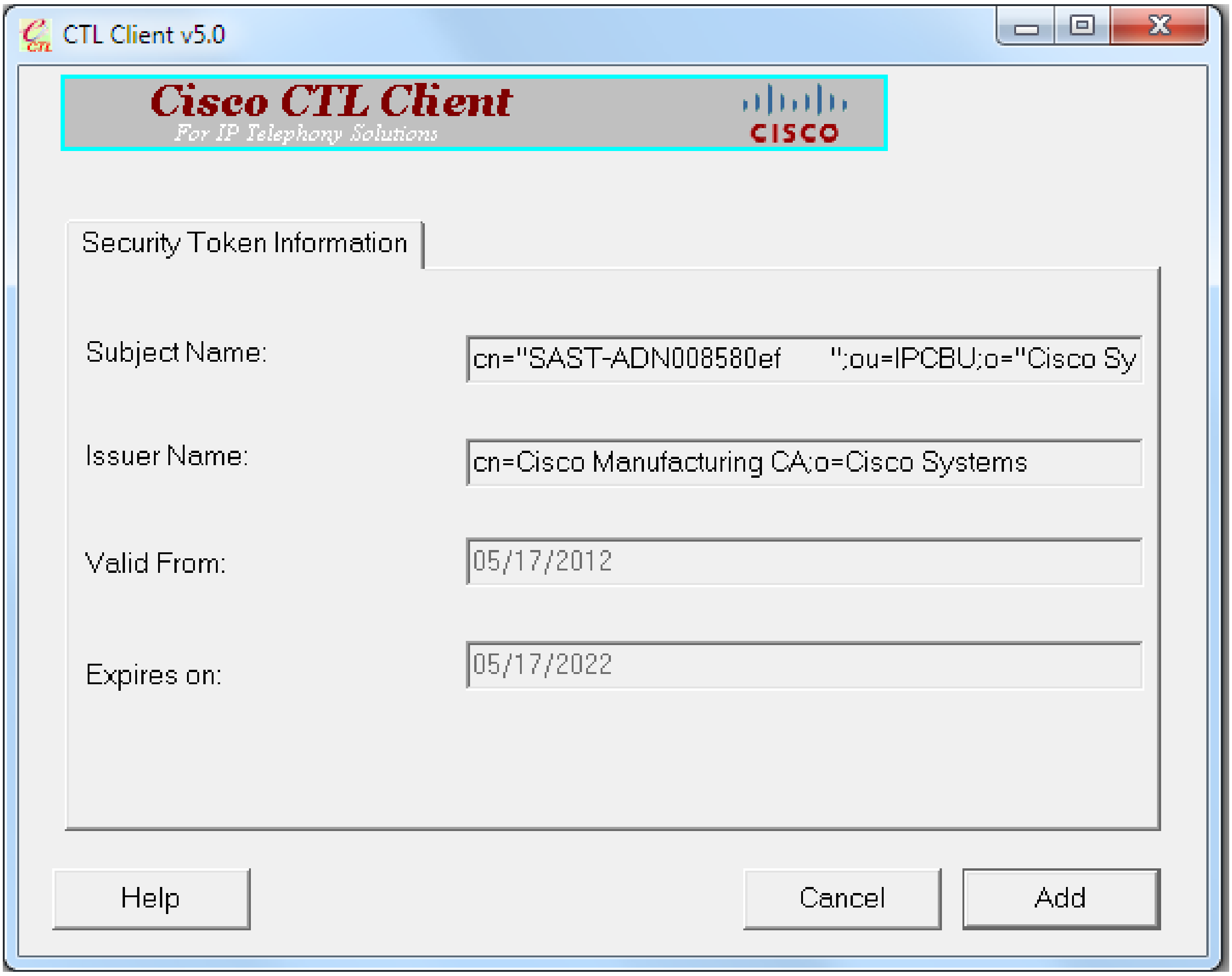
14. 插入第一个安全令牌，然后点击 OK（确定）：



CTLClient

Please insert a Security Token. Click Ok when done.

15. 系统显示安全令牌详细信息后，点击 Add（添加）：



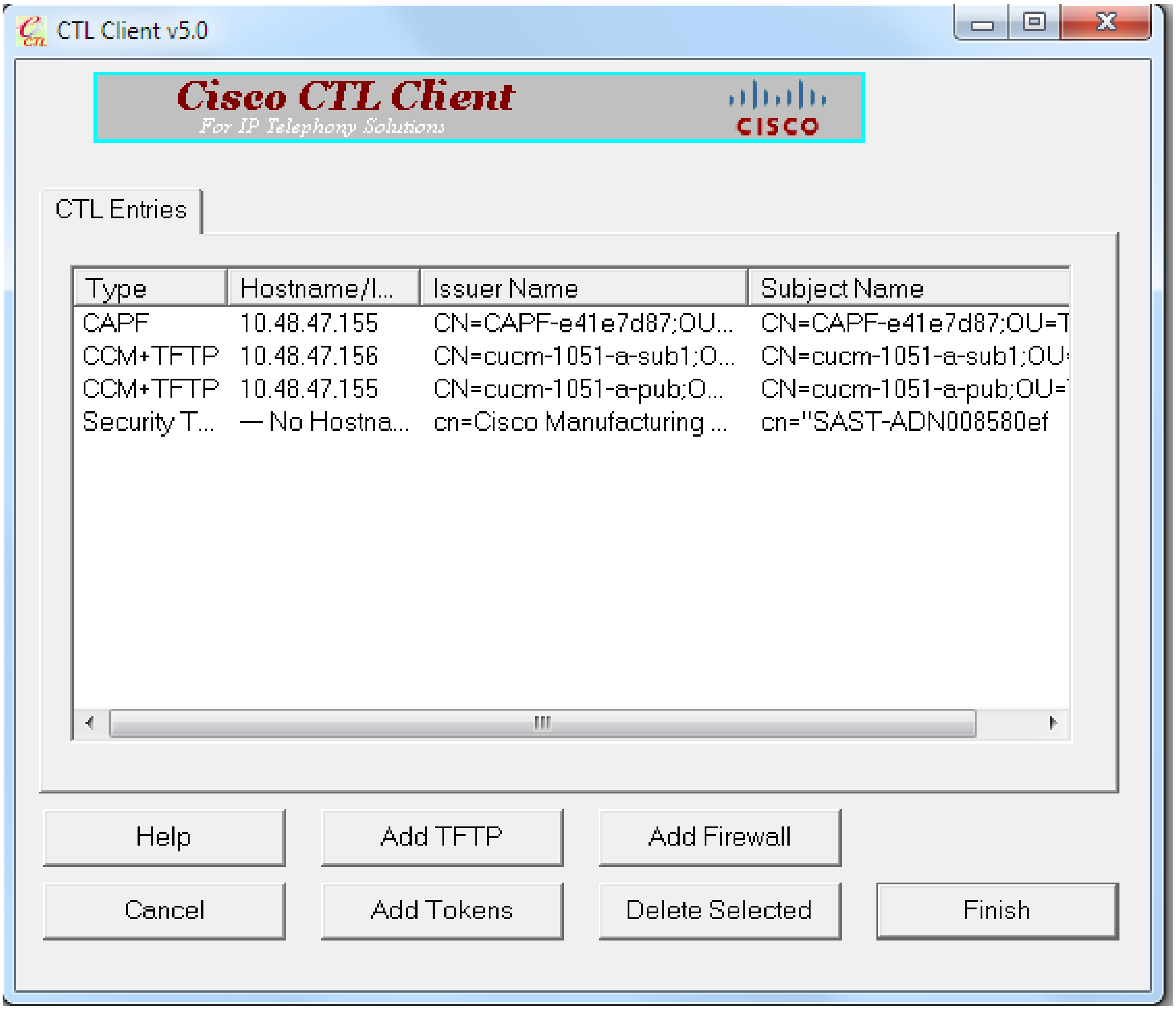
Subject Name: cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Sy

Issuer Name: cn=Cisco Manufacturing CA;o=Cisco Systems

Valid From: 05/17/2012

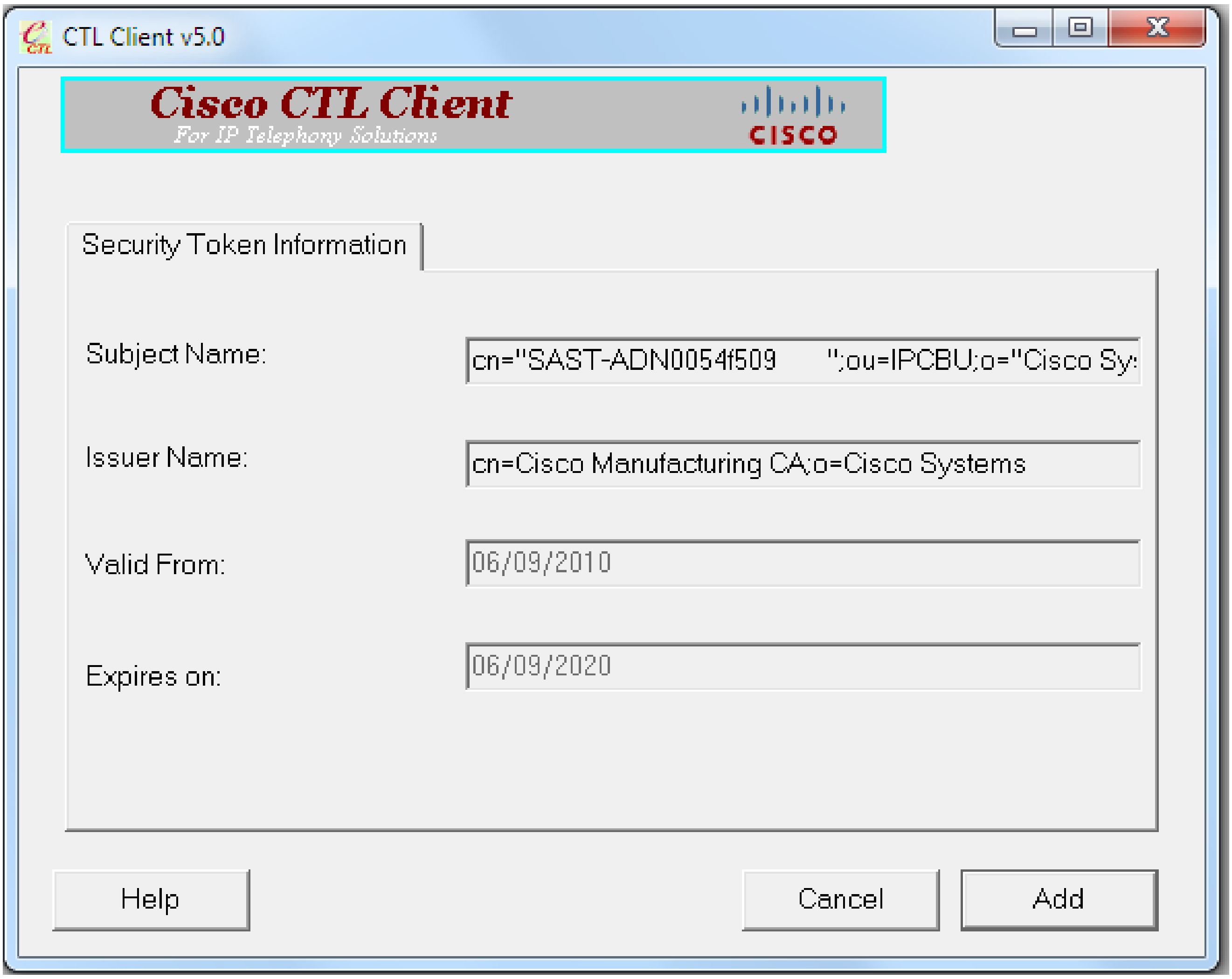
Expires on: 05/17/2022

16. 系统显示 CTL 文件的内容后，点击 Add Tokens（添加令牌）以添加第二个 USB 电子令牌：



Type	Hostname/I...	Issuer Name	Subject Name
CAPF	10.48.47.155	CN=CAPF-e41e7d87;OU...	CN=CAPF-e41e7d87;OU=T
CCM+TFTP	10.48.47.156	CN=cucm-1051-a-sub1;O...	CN=cucm-1051-a-sub1;OU
CCM+TFTP	10.48.47.155	CN=cucm-1051-a-pub;O...	CN=cucm-1051-a-pub;OU=
Security T...	— No Hostna...	cn=Cisco Manufacturing ...	cn="SAST-ADN008580ef

17. 系统显示安全令牌详细信息后，点击 Add（添加）：



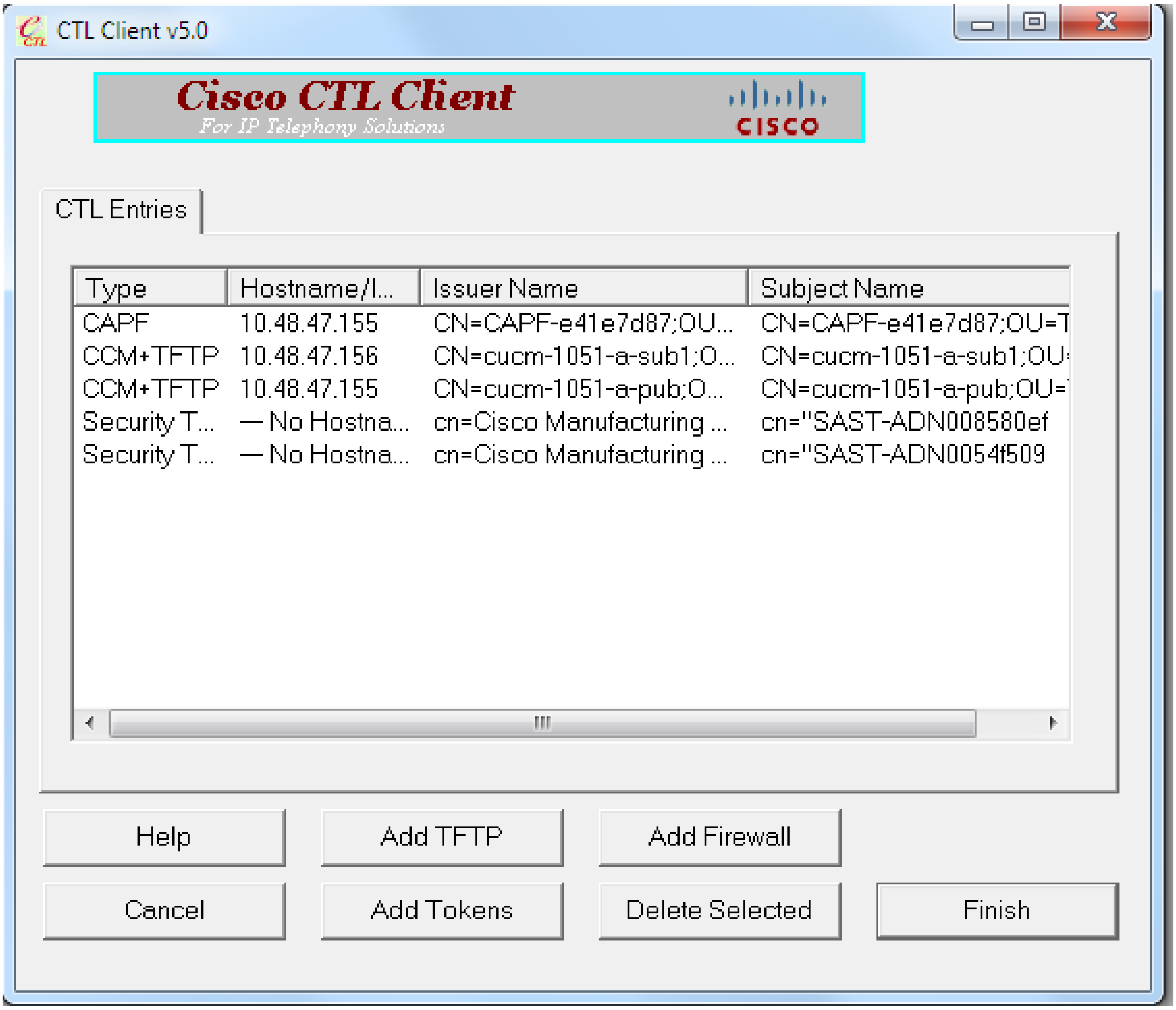
Subject Name: cn="SAST-ADN0054f509 ";ou=IPCBU;o="Cisco Sy:

Issuer Name: cn=Cisco Manufacturing CA;o=Cisco Systems

Valid From: 06/09/2010

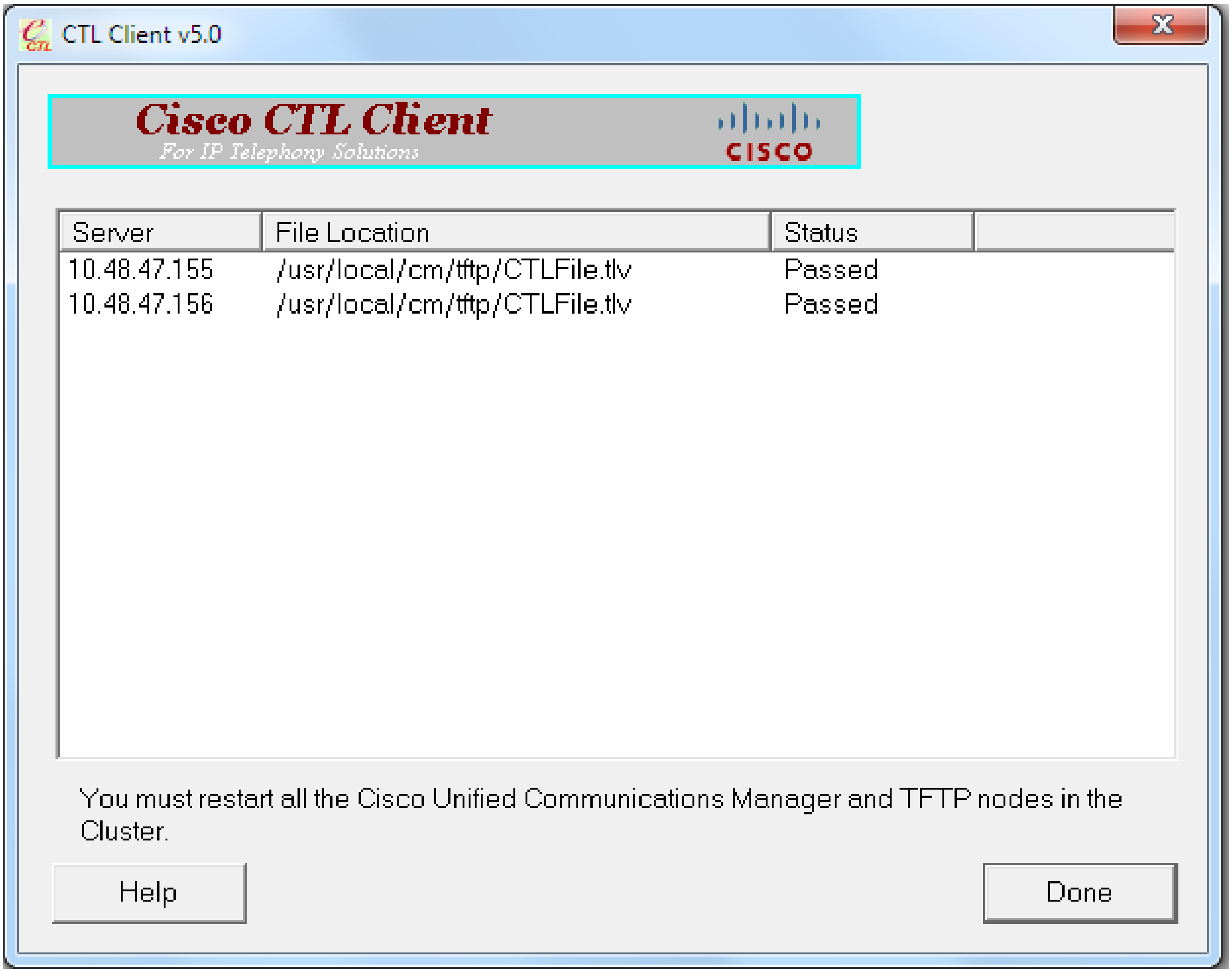
Expires on: 06/09/2020

18. 系统显示 CTL 文件的内容后，点击 Finish（完成）。当系统提示您输入密码时，请输入 Cisco123：



Type	Hostname/I...	Issuer Name	Subject Name
CAPF	10.48.47.155	CN=CAPF-e41e7d87;OU...	CN=CAPF-e41e7d87;OU=T
CCM+TFTP	10.48.47.156	CN=cucm-1051-a-sub1;O...	CN=cucm-1051-a-sub1;OU
CCM+TFTP	10.48.47.155	CN=cucm-1051-a-pub;O...	CN=cucm-1051-a-pub;OU=
Security T...	— No Hostna...	cn=Cisco Manufacturing ...	cn="SAST-ADN008580ef
Security T...	— No Hostna...	cn=Cisco Manufacturing ...	cn="SAST-ADN0054f509

19. 当系统显示存在 CTL 文件的 CUCM 服务器列表时，点击 Done（完成）：



Server	File Location	Status
10.48.47.155	/usr/local/cm/tftp/CTLFile.tlv	Passed
10.48.47.156	/usr/local/cm/tftp/CTLFile.tlv	Passed

You must restart all the Cisco Unified Communications Manager and TFTP nodes in the Cluster.

20. 在运行这些服务的集群中的所有节点上，重新启动 TFTP 和 CallManager 服务。

21. 重新启动所有 IP 电话，以便它们可以从 CUCM TFTP 服务获取新版本的 CTL 文件。

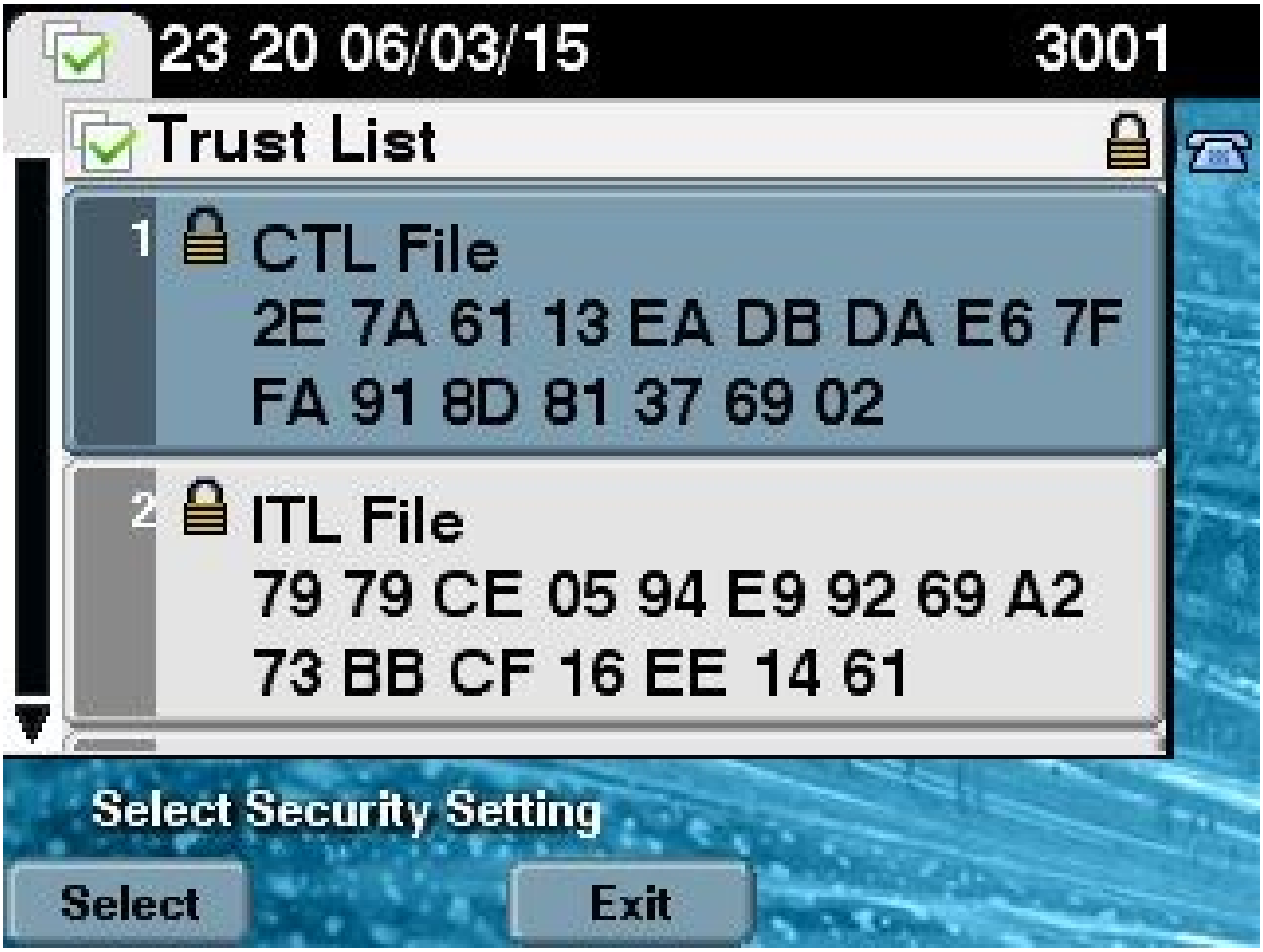
22. 要验证 CTL 文件的内容，请在 CLI 中输入 show ctl 命令。在 CTL 文件中，您可以看到两个 USB 电子令牌的证书（其中一个用于签署 CTL 文件）。以下为示例输出：

<#root>

```
admin:

show ctl


The checksum value of the CTL file:

2e7a6113eadbdae67ffa918d81376902(MD5)


d0f3511f10eef775cc91cce3fa6840c2640f11b8(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 22:53:33 CET 2015


[...]
```

```
CTL Record #:1
----
BYTEPOS TAG              LENGTH  VALUE
------- ---              ------  -----
1       RECORDLENGTH     2       1186
2       DNSNAME          1
3       SUBJECTNAME      56      cn="SAST-ADN0054f509 ";ou=IPCBU;o="Cisco Systems
4       FUNCTION         2

 System Administrator Security Token


5       ISSUERNAME       42      cn=Cisco Manufacturing CA;o=Cisco Systems
6       SERIALNUMBER     10

 3C:F9:27:00:00:00:AF:A2:DA:45


7       PUBLICKEY        140
9       CERTIFICATE      902     19 8F 07 C4 99 20 13 51 C5 AE BF 95 03 93 9F F2
                                 CC 6D 93 90 (SHA1 Hash HEX)
10      IPADDRESS        4
This etoken was not used to sign the CTL file.


[...]



CTL Record #:5
----
BYTEPOS TAG              LENGTH  VALUE
------- ---              ------  -----
1       RECORDLENGTH     2       1186
2       DNSNAME          1
3       SUBJECTNAME      56      cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4       FUNCTION         2

 System Administrator Security Token


5       ISSUERNAME       42      cn=Cisco Manufacturing CA;o=Cisco Systems
6       SERIALNUMBER     10

83:E9:08:00:00:00:55:45:AF:31


7       PUBLICKEY        140
9       CERTIFICATE      902     85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
                                 3E 8B 3A 4F (SHA1 Hash HEX)
10      IPADDRESS        4

This etoken was used to sign the CTL file.



The CTL file was verified successfully.
```

23. 在 IP 电话端，您可以验证重新启动 IP 电话后是否已下载更新的 CTL 文件版本（与 CUCM 的输出相比，MD5 校验和匹配）：



23 20 06/03/15 3001

Trust List

1 CTL File
2E 7A 61 13 EA DB DA E6 7F
FA 91 8D 81 37 69 02

2 ITL File
79 79 CE 05 94 E9 92 69 A2
73 BB CF 16 EE 14 61

Select Security Setting

可以进行此变更，因为您之前已将电子令牌证书导出并上传到 CUCM 证书信任存储区，并且 IP 电话能够验证该未知证书，该证书用于根据在 CUCM 上运行的信任验证服务 (TVS) 签署 CTL 文件。

此日志片段说明了 IP 电话如何与 CUCM TVS 通信，请求验证未知的电子令牌证书，该证书作为 Phone-SAST-trust 上传并受到信任：

<#root>

```
//

In the Phone Console Logs we can see a request sent to TVS server to verify unknown
 certificate


8074: NOT 23:00:22.335499 SECD: setupSocketToTvsProxy: Connected to TVS proxy server
8075: NOT 23:00:22.336918 SECD: tvsReqFlushTvsCertCache: Sent Request to TVS proxy,
 len: 3708

//

In the TVS logs on CUCM we can see the request coming from an IP Phone which is being
 successfully verified


23:00:22.052 | debug tvsHandleQueryCertReq
23:00:22.052 | debug tvsHandleQueryCertReq : Subject Name is: cn="SAST-ADN008580ef
 ";ou=IPCBU;o="Cisco Systems
23:00:22.052 | debug tvsHandleQueryCertReq : Issuer Name is: cn=Cisco Manufacturing
```

```
 CA;o=Cisco Systems
23:00:22.052 | debug tvsHandleQueryCertReq :subjectName and issuerName matches for
 eToken certificate
23:00:22.052 | debug tvsHandleQueryCertReq : SAST Issuer Name  is: cn=Cisco
 Manufacturing CA;o=Cisco Systems
23:00:22.052 | debug tvsHandleQueryCertReq : This is SAST eToken cert
23:00:22.052 | debug tvsHandleQueryCertReq : Serial Number is: 83E9080000005545AF31
23:00:22.052 | debug CertificateDBCache::getCertificateInformation - Looking up the
 certificate cache using Unique MAP ID : 83E9080000005545AF31cn=Cisco Manufacturing
 CA;o=Cisco Systems
23:00:22.052 | debug ERROR:CertificateDBCache::getCertificateInformation - Cannot find
 the certificate in the cache
23:00:22.052 | debug CertificateCTLCache::getCertificateInformation - Looking up the
 certificate cache using Unique MAP ID : 83E9080000005545AF31cn=Cisco Manufacturing
 CA;o=Cisco Systems, len : 61
23:00:22.052 | debug CertificateCTLCache::getCertificateInformation - Found entry
 {rolecount : 1}
23:00:22.052 | debug CertificateCTLCache::getCertificateInformation - {role : 0}
23:00:22.052 | debug convertX509ToDER -x509cert : 0xa3ea6f8
23:00:22.053 | debug tvsHandleQueryCertReq: Timer started from tvsHandleNewPhConnection

//

In the Phone Console Logs we can see reply from TVS server to trust the new certificate
 (eToken Certificate which was used to sign the CTL file)


8089: NOT 23:00:22.601218 SECD: clpTvsInit: Client message received on TVS proxy socket
8090: NOT 23:00:22.602785 SECD: processTvsClntReq: Success reading the client TVS
 request, len : 3708
8091: NOT 23:00:22.603901 SECD: processTvsClntReq: TVS Certificate cache flush
 request received
8092: NOT 23:00:22.605720 SECD: tvsFlushCertCache: Completed TVS Certificate cache
 flush request
```

为无令牌 CTL 解决方案重新生成证书

本节介绍使用无令牌 CTL 解决方案时如何重新生成 CUCM 集群安全证书。

在 CUCM 维护过程中，有时会变更 CUCM 发布方节点 CallManager 证书。

可能发生这种情况的场景包括主机名变更、域变更或者仅重新生成证书（由于接近证书到期日期）。

更新 CTL 文件后，使用与 IP 电话上安装的 CTL 文件中不同的证书进行签署。

通常，不接受这个新的CTL文件；但是，在IP电话找到用于签署CTL文件的未知证书后，它将联系CUCM上的TVS服务。

注意：TVS服务器列表位于IP电话配置文件中，并且从IP电话设备池> CallManager组映射到CUCM服务器。

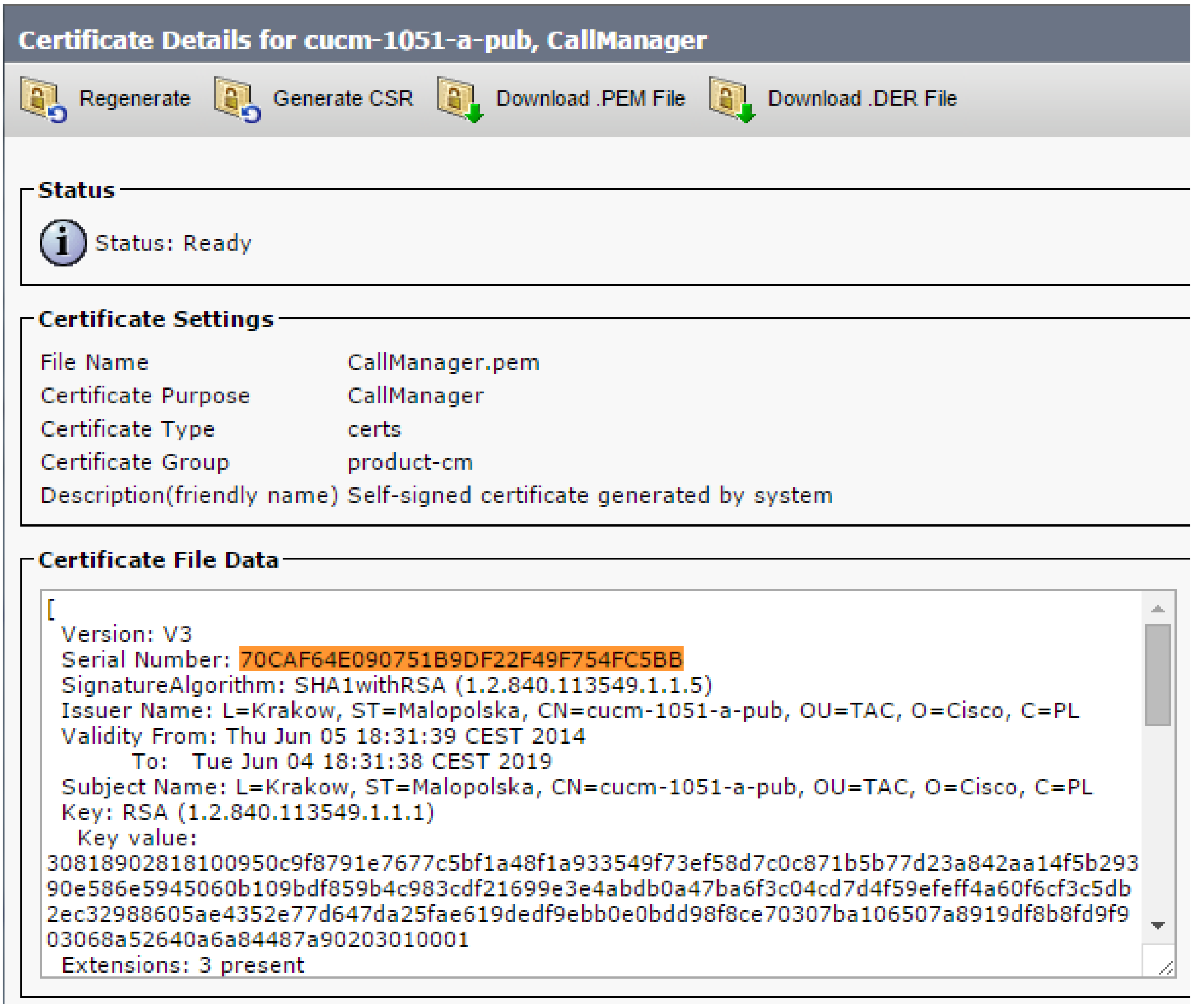
成功验证 TVS 服务器后，IP 电话会使用新版本更新其 CTL 文件。在以下场景下，会发生此类事件：

1. CUCM 和 IP 电话上存在 CTL 文件。CUCM 发布方节点的 CCM+TFT（服务器）证书用于签署 CTL 文件：

<#root>

```
admin:

show ctl


The checksum value of the CTL file:

7b7c10c4a7fa6de651d9b694b74db25f(MD5)


819841c6e767a59ecf2f87649064d8e073b0fe87(SHA1)

Length of CTL file: 4947
The CTL File was last modified on Mon Mar 09 16:59:43 CET 2015


[...]



        CTL Record #:1
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1156
2       DNSNAME         16

cucm-1051-a-pub


3       SUBJECTNAME     62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
4       FUNCTION        2

System Administrator Security Token


5       ISSUERNAME      62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
6       SERIALNUMBER    16

70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB


7       PUBLICKEY       140
8       SIGNATURE       128
9       CERTIFICATE     694     E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D
                                21 A5 A3 8C 9C (SHA1 Hash HEX)
10      IPADDRESS       4

This etoken was used to sign the CTL file.



CTL Record #:2
----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
```

```
1       RECORDLENGTH    2       1156
2       DNSNAME         16

cucm-1051-a-pub


3       SUBJECTNAME     62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
4       FUNCTION        2

CCM+TFTP


5       ISSUERNAME      62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
6       SERIALNUMBER    16

70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB


7       PUBLICKEY       140
8       SIGNATURE       128
9       CERTIFICATE     694     E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D
                                21 A5 A3 8C 9C (SHA1 Hash HEX)
10      IPADDRESS       4

[...]


The CTL file was verified successfully.
```



Status

Status: Ready

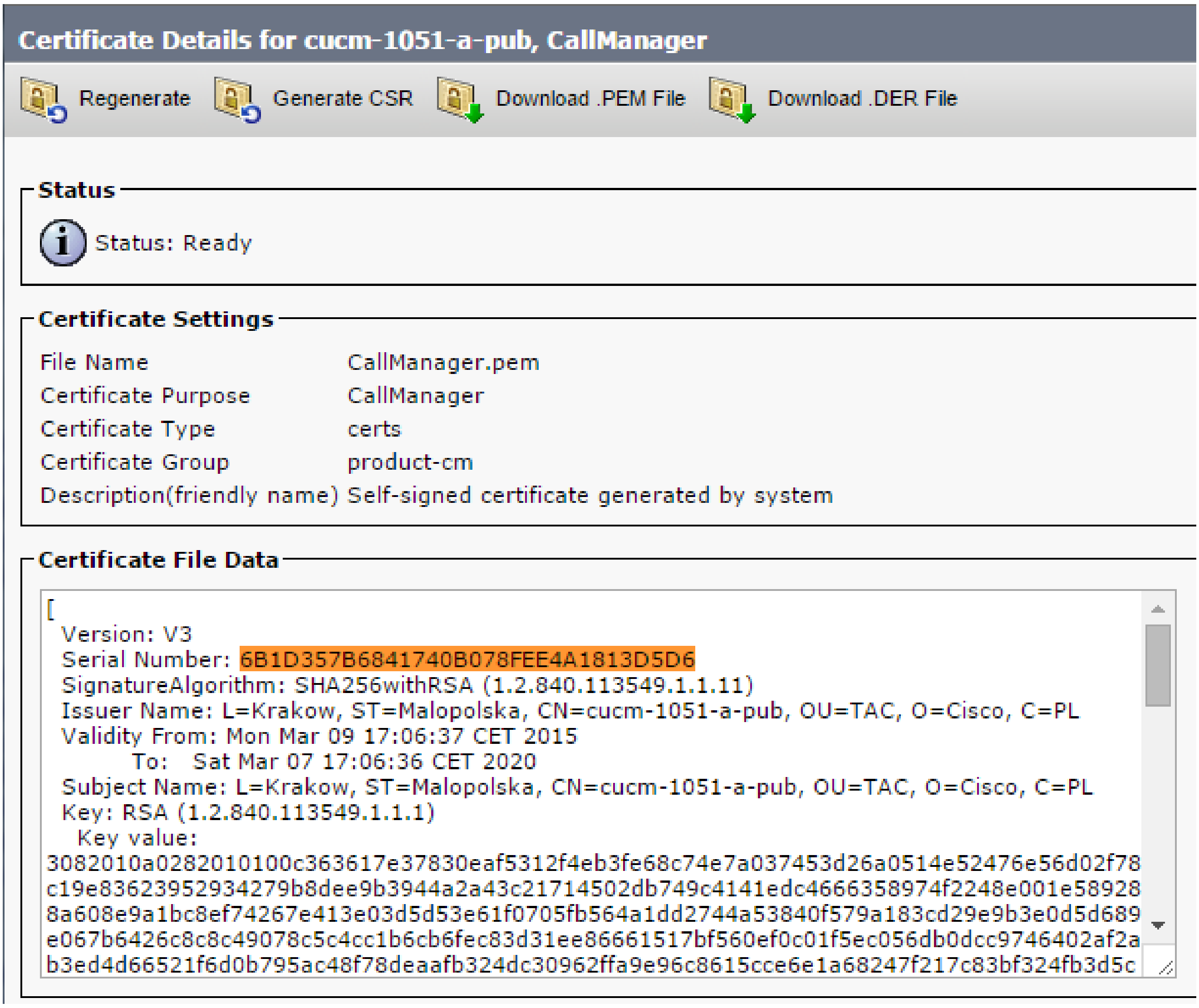
Certificate Settings

File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Self-signed certificate generated by system

Certificate File Data

```
[
  Version: V3
  Serial Number: 70CAF64E090751B9DF22F49F754FC5BB
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: L=Krakow, ST=Malopolska, CN=cucm-1051-a-pub, OU=TAC, O=Cisco, C=PL
  Validity From: Thu Jun 05 18:31:39 CEST 2014
          To:   Tue Jun 04 18:31:38 CEST 2019
  Subject Name: L=Krakow, ST=Malopolska, CN=cucm-1051-a-pub, OU=TAC, O=Cisco, C=PL
  Key: RSA (1.2.840.113549.1.1.1)
    Key value:
30818902818100950c9f8791e7677c5bf1a48f1a933549f73ef58d7c0c871b5b77d23a842aa14f5b293
90e586e5945060b109bdf859b4c983cdf21699e3e4abdb0a47ba6f3c04cd7d4f59efeff4a60f6cf3c5db
2ec32988605ae4352e77d647da25fae619dedf9ebb0e0bdd98f8ce70307ba106507a8919df8b8fd9f9
03068a52640a6a84487a90203010001
  Extensions: 3 present
```

2. CallManager.pem 文件（CCM+TFTP 证书）已重新生成，您可以看到证书的序列号已更改：



Status

Status: Ready

Certificate Settings

File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Self-signed certificate generated by system

Certificate File Data

```
[
  Version: V3
  Serial Number: 6B1D357B6841740B078FEE4A1813D5D6
  SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
  Issuer Name: L=Krakow, ST=Malopolska, CN=cucm-1051-a-pub, OU=TAC, O=Cisco, C=PL
  Validity From: Mon Mar 09 17:06:37 CET 2015
           To:   Sat Mar 07 17:06:36 CET 2020
  Subject Name: L=Krakow, ST=Malopolska, CN=cucm-1051-a-pub, OU=TAC, O=Cisco, C=PL
  Key: RSA (1.2.840.113549.1.1.1)
    Key value:
3082010a0282010100c363617e37830eaf5312f4eb3fe68c74e7a037453d26a0514e52476e56d02f78
c19e83623952934279b8dee9b3944a2a43c21714502db749c4141edc4666358974f2248e001e58928
8a608e9a1bc8ef74267e413e03d5d53e61f0705fb564a1dd2744a53840f579a183cd29e9b3e0d5d689
e067b6426c8c8c49078c5c4cc1b6cb6fec83d31ee86661517bf560ef0c01f5ec056db0dcc9746402af2a
b3ed4d66521f6d0b795ac48f78deaafb324dc30962ffa9e96c8615cce6e1a68247f217c83bf324fb3d5c
```

3. 在 CLI 中输入 utils ctl update CTLFile 命令，以更新 CTL 文件：

<#root>

```
admin:

utils ctl update CTLFile


This operation updates the CTLFile. Do you want to continue? (y/n):y

Updating CTL file
CTL file Updated
Please Restart the TFTP and Cisco CallManager services on all nodes in
 the cluster that run these services
admin:
```

4. TVS 服务使用新的 CTL 文件详细信息更新其证书缓存：

<#root>

```
17:10:35.825 | debug CertificateCache::localCTLCacheMonitor -

CTLFile.tlv has been
 modified

. Recaching CTL Certificate Cache
17:10:35.826 | debug updateLocalCTLCache :

Refreshing the local CTL certificate cache


17:10:35.827 | debug tvs_sql_get_all_CTL_certificate - Unique Key used for Caching ::


6B1D357B6841740B078FEE4A1813D5D6

CN=

cucm-1051-a-pub

;OU=TAC;O=Cisco;L=Krakow;
 ST=Malopolska;C=PL, length : 93
17:10:35.827 | debug tvs_sql_get_all_CTL_certificate - Unique Key used for Caching ::


6B1D357B6841740B078FEE4A1813D5D6

CN=

cucm-1051-a-pub

;OU=TAC;O=Cisco;L=Krakow;
 ST=Malopolska;C=PL, length : 93
17:10:35.827 | debug tvs_sql_get_all_CTL_certificate - Unique Key used for Caching ::
 744B5199770516E799E91E81D3C8109BCN=CAPF-e41e7d87;OU=TAC;O=Cisco;L=Krakow;
 ST=Malopolska;C=PL, length : 91
17:10:35.827 | debug tvs_sql_get_all_CTL_certificate - Unique Key used for Caching ::
 6BEBFDCDCD8CA277CB2FD1D183A60E72CN=cucm-1051-a-sub1;OU=TAC;O=Cisco;L=Krakow;
 ST=Malopolska;C=PL, length : 94
```

5. 查看 CTL 文件内容时，您可以看到该文件已使用发布方节点的新 CallManager 服务器证书签署：

<#root>

```
admin:

show ctl


The checksum value of the CTL file:

ebc649598280a4477bb3e453345c8c9d(MD5)


ef5c006b6182cad66197fac6e6530f15d009319d(SHA1)

Length of CTL file: 6113
The CTL File was last modified on Mon Mar 09 17:07:52 CET 2015


[..]
```

```
         CTL Record #:1
              ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1675
2       DNSNAME         16

cucm-1051-a-pub


3       SUBJECTNAME     62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
4       FUNCTION        2

System Administrator Security Token


5       ISSUERNAME      62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
6       SERIALNUMBER    16

6B:1D:35:7B:68:41:74:0B:07:8F:EE:4A:18:13:D5:D6


7       PUBLICKEY       270
8       SIGNATURE       256
9       CERTIFICATE     955     5C AF 7D 23 FE 82 DB 87 2B 6F 4D B7 F0 9D D5
                                86 EE E0 8B FC (SHA1 Hash HEX)
10      IPADDRESS       4


This etoken was used to sign the CTL file.



         CTL Record #:2
              ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1675
2       DNSNAME         16

cucm-1051-a-pub


3       SUBJECTNAME     62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
4       FUNCTION        2

CCM+TFTP


5       ISSUERNAME      62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                ST=Malopolska;C=PL
6       SERIALNUMBER    16

6B:1D:35:7B:68:41:74:0B:07:8F:EE:4A:18:13:D5:D6


7       PUBLICKEY       270
8       SIGNATURE       256
9       CERTIFICATE     955     5C AF 7D 23 FE 82 DB 87 2B 6F 4D B7 F0 9D D5
                                86 EE E0 8B FC (SHA1 Hash HEX)
```

```
10      IPADDRESS       4

[...]


The CTL file was verified successfully.
```

6. 在“Unified Serviceability”页面中，在运行这些服务的集群中所有节点上，重新启动 TFTP 和 Cisco CallManager 服务。

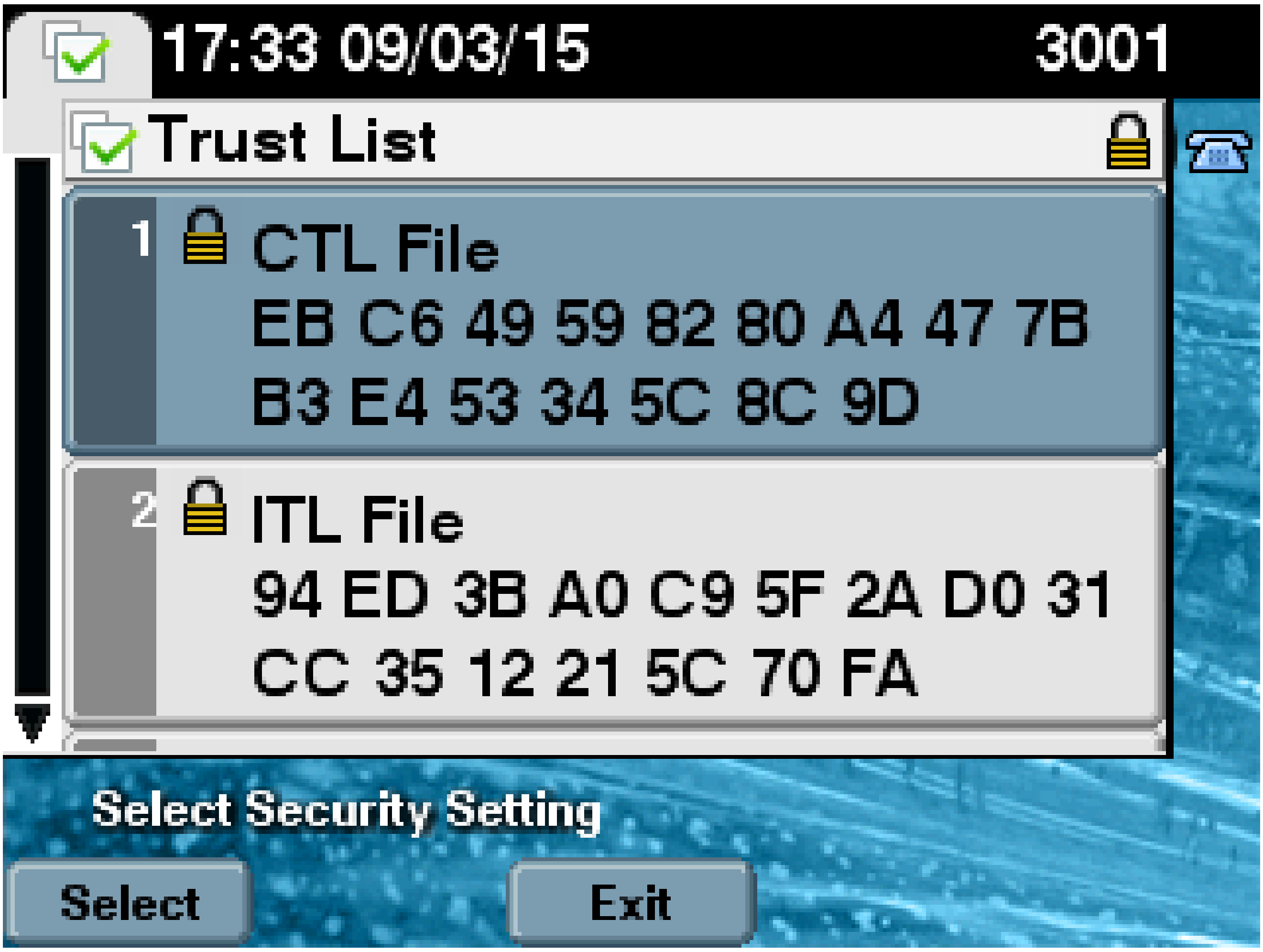
7. IP 电话已重新启动并联系 TVS 服务器，以验证当前用于签署新版本 CTL 文件的未知证书：

<#root>

```
//

In the Phone Console Logs we can see a request sent to TVS server to verify
 unknown certificate


2782: NOT 17:21:51.794615 SECD: setupSocketToTvsProxy: Connected to TVS proxy server
2783: NOT 17:21:51.796021 SECD: tvsReqFlushTvsCertCache: Sent Request to TVS
 proxy, len: 3708

//

In the TVS logs on CUCM we can see the request coming from an IP Phone which is
 being successfully verified


17:21:51.831 |   debug tvsHandleQueryCertReq
17:21:51.832 |   debug tvsHandleQueryCertReq : Subject Name is: CN=cucm-1051-a-pub;
 OU=TAC;O=Cisco;L=Krakow;ST=Malopolska
17:21:51.832 |   debug tvsHandleQueryCertReq : Issuer Name is: CN=cucm-1051-a-pub;
 OU=TAC;O=Cisco;L=Krakow;ST=Malopolska;
17:21:51.832 |   debug tvsHandleQueryCertReq : Serial Number is:
 6B1D357B6841740B078FEE4A1813D5D6
17:21:51.832 |   debug CertificateDBCache::getCertificateInformation - Looking up the
 certificate cache using Unique MAPco;L=Krakow;ST=Malopolska;C=PL
17:21:51.832 |   debug CertificateDBCache::getCertificateInformation - Found entry
 {rolecount : 2}
17:21:51.832 |   debug CertificateDBCache::getCertificateInformation - {role : 0}
17:21:51.832 |   debug CertificateDBCache::getCertificateInformation - {role : 2}
17:21:51.832 |   debug convertX509ToDER -x509cert : 0xf6099df8
17:21:51.832 |   debug tvsHandleQueryCertReq: Timer started from
 tvsHandleNewPhConnection

//

In the Phone Console Logs we can see reply from TVS server to trust the new
 certificate (new CCM Server Certificate which was used to sign the CTL file)


2797: NOT 17:21:52.057442 SECD: clpTvsInit: Client message received on TVS
 proxy socket
2798: NOT 17:21:52.058874 SECD: processTvsClntReq: Success reading the client TVS
 request, len : 3708
2799: NOT 17:21:52.059987 SECD: processTvsClntReq: TVS Certificate cache flush
```

```
 request received
2800: NOT 17:21:52.062873 SECD: tvsFlushCertCache: Completed TVS Certificate
 cache flush request
```

8. 最后，在 IP 电话上，您可以验证是否已使用新版本更新 CTL 文件，以及新 CTL 文件的 MD5 校验和是否与 CUCM 的校验和匹配：



17:33 09/03/15 3001

Trust List

1 CTL File
EB C6 49 59 82 80 A4 47 7B
B3 E4 53 34 5C 8C 9D

2 ITL File
94 ED 3B A0 C9 5F 2A D0 31
CC 35 12 21 5C 70 FA

Select Security Setting

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。